

TDK DOLGOZAT

Szerző: Molnár Balázs

Adatgyűjtés az okostelefonok világában

Tudományos Diákköri Dolgozat

Témavezető: Pintér Róbert
Egyetemi Adjunktus

Molnár Balázs

Budapesti Corvinus Egyetem

Gazdálkodástudományi Kar

Infokommunikációs Tanszék

Gazdaságinformatikus Szak

III. évfolyam

2013. 03. 25.

Tartalomjegyzék

1. BEVEZETÉS.....	1
1.1 A téma bemutatása	1
1.2 A dolgozat felépítése	2
2. OKOSTELEFONOK.....	3
3. BIZTONSÁGOS?	4
4. ADATGYŰJTÉSI VESZÉLYEK.....	5
4.1 Geolokáció alapú támadás	6
4.2 Engedélyek problémái.....	6
4.3 Alkalmazás okozta sebezhetőség.....	6
4.4 Nem biztonságos WIFI használata	7
4.4.1 WIFI hackelés.....	8
4.5 Eltulajdonított vagy elvesztett készülékek.....	10
5. KÜLÖNBÖZŐ PLATFORMOK ÉS MOBILSZOLGÁLTATÓK ADATGYŰJTÉSI ELJÁRÁSAI.....	10
6. FOGYASZTÓI ÉRDEKVÉDELMI SZERVEZETEK ÉS MUNKÁSSÁGUK.....	12
6.1 Electronic Frontier Foundation.....	12
6.2 Federal Trade Commission	14
6.3 Aktualitás	15
7. ALKALMAZÁSOK	16
7.1 Mi alapján döntünk?.....	16
7.2 Ha nem pénzt, akkor mit adunk cserébe?	16
7.2.1 Hirdetések.....	17
7.2.2 Demó verziók.....	17
7.2.3 Alkalmazáson belüli vásárlás lehetősége	17
7.3 Programok névjegyzék gyűjtése	18
7.4 Engedélyek kijátszhatósága	20
7.5 Alkalmazások összehasonlítása	20
7.6 Aktualitás	23
8. GEOLOKÁCIÓS KUTATÁS.....	24
9. VÉDELMI LEHETŐSÉGEK.....	29
9.1 Megelőzés.....	29
9.2 Védelem nyílt WIFI hálózaton is	30
9.3 Céges adatok biztonsága.....	30
10. AZ ADATGYŰJTÉS POZITÍV OLDALAI.....	31
10.1 Geolokáció.....	31
10.1.1 Forgalmi információk.....	31
10.1.2 Lopott autók felderítése	32
10.1.3 Egyéb	32
10.2 Fertőző betegségek terjedésének megíjósolhatósága.....	32
10.3 Nemzetközi kutatás Szegeden.....	33

11. ÖSSZEFOGLALÁS	33
Irodalomjegyzék.....	36
A dolgozatban hivatkozott okostelefon alkalmazások	39
Melléklet	41
1. számú melléklet: Alkalmazások összehasonlítása.....	41
2. számú melléklet: Kutatási anyagok.....	42
2.1 Férfi ismerős adatai	42
2.2 Nő ismerős adatai	44

1. BEVEZETÉS

1.1 A téma bemutatása

Napjainkban a technika rohamos ütemben fejlődik. Egymást követik az újabb, modernebb termékek és szolgáltatások, ezáltal a folyamat követhetlenné válik. Korosztályom több-kevesebb sikerrel próbálja felvenni ezt a gyors haladási iramot, melybe beleszületett. Számos elektronikai cikk életünk részévé vált, létezésük nélkül el sem tudnánk képzelni mindennapjainkat. Rengeteg pozitív érv sorakoztatható fel mellettük, azonban sokan elfeledkeznek arról, hogy ezen eszközök használatának negatív oldalával is számolni kell. Az Internet valamint az erre épülő termékek, a fogyasztókkal szembeni károkozás kulcsfontosságú eszközeivé váltak az évek folyamán. Folyamatosan kerülnek napvilágot különböző visszaélésekből eredő jogi viták, illetve a fogyasztói érdekvédelmi szervezetek erőfeszítései is egyre nagyobb szerepet kapnak a médiában. Az okostelefonok kitüntetett pozícióban helyezkednek el ezen a téren. Egyfajta forradalomról beszélhetünk, ahol a mobilkészülékek az átlagosnál gyorsabban fejlődnek, az eladott termékek darabszáma pedig folyamatos ütemben növekszik.

Gazdaságinformatikusként, valamint a Magyar Telekom Nyrt. távközlési és telekommunikációs vállalat dolgozójaként, gazdasági és technikai szempontból is vizsgálom ezeket az eszközöket. A biztonság fontossága megkérdőjelezhetetlen, melyet én mindig is kitüntetett helyen kezeltem. A tárgyban való jártasságom alapjául szolgálnak korábbi tanulmányaim. Korszerű IT biztonságtechnika szemináriumon felkeltették az érdeklődésemet a különböző adathalászati eszközök iránt, később pedig mikor megkaptam első, azóta is használt okostelefonomat elhatároztam, hogy mélyebbre ások a témában. Végül John M. Simpson, az amerikai jogok szószólójának idézete: „*These aren't smartphones – they are spy phones*”¹ (idézi May - Wolverton 2011) terelt a TDK írás útjára.

Nehezítette a kutatást, hogy viszonylag friss termékről illetve szolgáltatásról beszélhetünk, ezáltal aránylag kevés irodalom áll rendelkezésre. Habár itthon is rengetegen foglalkoznak a témával, tényadatokat és aktuális tudnivalókat legfőképpen

¹ „Ezek nem okostelefonok – ezek kém telefonok”

külföldi weblapokról, szakmai fórumokról tudtam beszerezni. Ennek ellenére nagy örömet leltem a dolgozat elkészítésében. Kutatásaim és felfedezéseim folyamatos munkára ösztönöztek.

Több kérdés is felmerült bennem a témával kapcsolatban, melynek utánajárván megpróbáltam korrekt, valós és friss információkkal szolgálni. Kíváncsi voltam, hogy milyen adatok gyűjthetők a felhasználóról, mobilkészülékén keresztül. Ezen információk megszerzése milyen üzleti lehetőségeket rejt, illetve jelenthet-e versenyelőnyt. Továbbá, hogy a fogyasztói érdekvédelmi szervezetek mit tesznek a felhasználók védelme érdekében. Illetve, hogy az adatgyűjtésnek milyen pozitív oldalai vannak.

Fő kutatási kérdésként a lehetséges visszaéléseket vizsgáltam, illetve, hogy mire figyeljen egy mai okostelefon felhasználó.

1.2 A dolgozat felépítése

Dolgozatom témájául tehát az okosostelefónia világában történő adatgyűjtést választottam. Főként geolokációs alapokra fektetem a hangsúlyt, mivel ez az a plusz, amire mind a szolgáltatók, mind a visszaélést elkövetők kíváncsiak. Amíg a PC-k korszakában viszonylag helyhez kötött használatról beszélhetünk, addig az okostelefónia világában folyamatos mozgásunk figyelhető meg. Koordinációs adataink pedig számtalan új szolgáltatást és visszaélési lehetőséget rejtenek. Dolgozatommal azt szerettem volna elérni, hogy egy olyan munkát adjak ki a kezemből, amely hasznára válik a mai okostelefont használó társadalomnak.

Kezdeként egy rövid történelmi áttekintéssel kezdődik. Ezt követően különböző – az okostelefonok világában alkalmazandó – adatgyűjtési technikákat járok körbe. Ezután a legnagyobb platformok és mobilszolgáltatók információszerzési eljárásainak előnyeit és hátrányait ismertetem. Majd nagy fogyasztói érdekvédelmi szervezetek és tevékenységük bemutatása következik. Az ez utáni fejezetben konkrét alkalmazások összehasonlítása és vizsgálata történik, valamint a gyermekeket fenyegető veszélyekről számolok be. Ezt követően kutatásomat mutatom be, melynek tartalma, érzékeny információk feltárása okostelefon segítségével. Egy hetes adatokat monitorozok, főként geolokáció alapján, két kedves ismerősöm mobilkészüléke segítségével. Majd az így kapott értékeket elemzem és következtetéseket vonok le

belőlük. Végül védelmi lehetőségeket ismertettek, valamint az adatgyűjtés pozitív oldalát, illetve az esetleges jövőbeni irányokat.

TDK dolgozatom célja tehát, hogy az olvasó mélyebb ismereteket szerezzen az adathalászattal kapcsolatban. Felismerje az okostelefon használat veszélyeit, fenyegetettségét. Derítse fel és alkalmazza készüléke adottságait, azonban tegye meg a szükséges biztonsági lépéseket adatai védelme érdekében.

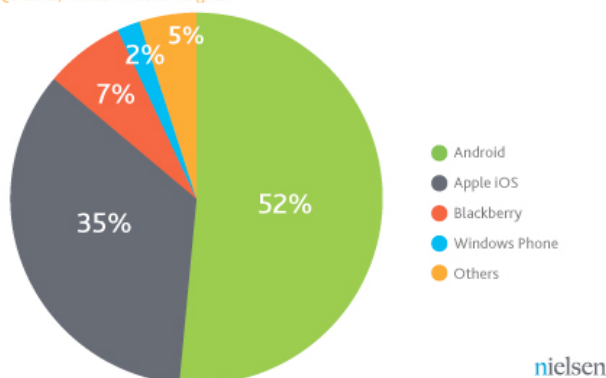
2. OKOSTELEFONOK

Mielőtt bármilyen mélyen szántó állításokat szemléltetnék, tisztázni kell, hogy mit értünk okostelefon alatt. „Az okostelefonok olyan fejlett, gyakran **számítógépszerű** funkciókkal is felszerelt telefonok, amelyek a **telefonáláson kívül** számos egyéb funkcióval is rendelkeznek: különféle **alkalmazások tölthetők le**, és telepíthetők rájuk; **e-mail és internethasználatra is alkalmasak**; általában **érintőképernyővel vagy teljes** **ábécét is tartalmazó (ún. QWERTY) billentyűzettel rendelkeznek**” (Pintér 2011a; kiemelés az eredetiben).

A fogalom tisztázása után, egy rövid történelmi áttekintés következik. A Strategy Analytics piackutatásából kiderült, hogy 2012 harmadik negyedévében az okostelefonnal rendelkező felhasználók száma átlépte az 1 milliárd főt (Gálffy 2012). A kutatás kiemeli, hogy az okostelefonok piaca 1996-ban indult el egy Nokia eszközzel. Ezt több szakértő is cáfolja. Sokan az 1992-ben bemutatott IBM Simont tartják az okostelefónia első készülékének. Egy biztos, a Nokia dobta piacra az első olyan eszközt, amely teljes PDA funkcionalitást kínált e-mailezéssel, valamint textwebes böngészéssel. (Szilágyi 2011) Természetesen ez nyomdokaiba sem léphetett a mai tudásszintnek. A nagy áttörést azonban az iPhone és Android megjelenése hozta el 2007 illetve 2008-ban.

Tehát a Nokia még az ezredforduló előtt felismerte ezen készülékek szükségességét, valamint meglátta a bennük rejlő lehetőséget. Az akkor még csak felsorakoztatott álmok – mint például az online bankolás vagy tőzsdézés lehetősége – ma már mindennapjaink részét képezik. Ennek tudatában megdöbbentő a tény, hogy a Nokia Windows Phone telefonjai csupán 2% piaci részesedést érnek el Amerikában (Nielsen 2012), és ez az arány világszerte megfigyelhető.

Top U.S. Smartphone Operating Systems by Market Share
Q3 2012, Nielsen Mobile Insights



Forrás: Nielsen 2012

Az okostelefonok eladásának folyamatos növekedéséről beszélhetünk Magyarországon is. Az NRC 2012-es felmérése alapján: Az internethasználók 42%-ának van okostelefonja, vagy okostelefon funkciókkal bővített hordozható eszköze. (Klenovszki 2012). A telepíthető alkalmazások tárháza pedig kifogyhatatlan.

3. BIZTONSÁGOS?

Az átlag felhasználó biztonságban érzi magát. Csak az adott operációs rendszerhez tartozó online áruházból tölt le alkalmazásokat, filmeket, zenét. Leveleit olvassa, szörföl az Interneten, közösségi szájtokon aktívan tevékenykedik, játszik és természetesen telefonál készülékén. Azt hisszük, hogy veszélytelen az okostelefonok mindennapi használata, azonban – mint majd azt dolgozatomban bemutatásra kerül – a gyakorlat nem ezt igazolja. A Sophos biztonsági szoftverfejlesztő cégnél, vezető technikus beosztásban dolgozó James Lyne szavaival élve: *“Jelenleg nem rendelkezünk a megfelelő biztonsági aggodalommal és paranoiával a mobil eszközökkel kapcsolatban”* ebből kifolyólag *“Amíg a felhasználók úgy vélik, hogy ezek a mobil eszközök varázslatosan biztonságosak, sokkal nagyobb valószínűséggel válnak klasszikus támadás áldozatává”*. (idézi Search Security 2011 saját fordítás) Tehát, sokkal nagyobb hangsúlyt kell fordítanunk adataink védelmére, mint azt gondolnánk.

Az Internetes történő, adatokkal való visszaélés kiterjed online állapotban lévő fejlett okostelefonjainkra is. A Norton 2012-es Cybercrime Report-jának tényadataival jól szemléltethető a védelem szükségessége. A felmérésben 24 ország 13.018 felnőttje

vett részt 18-64 életév között. A múlt évben 46%-uk vált Internetes bűnözés áldozatává. A kockázati tényezők között szerepel, hogy mobilkészülékükön egyre több online forgalmat generálnak, minthogy 63%-uk rendszeresen követi a közösségi szájtok történéseit, 31%-uk vásárol online, 67%-uk intézi levelezését és 24%-uk banki tranzakciókat folytat okostelefonján. A 35%-uknak pedig tűnt már el mobiltelefonja (Norton 2012). A megszerzett információk számtalan visszaélési lehetőséget nyújtanak.

Egy jól működő, névvel ellátott email címlista segítségével, spam üzenetek küldhetők. Az levél tartalma személyessé tehető, ezáltal a gyanútlan felhasználó könnyedén bedől a játékfelhívásnak vagy termékajánlásnak. Monitorozott GPS adatok által tudható, hogy mikor nem tartózkodunk otthon, ami nagy segítséget nyújthat illetéktelen személyeknek lakhelyünkön történő bűncselekmény elkövetésére. Bizalom hiányában, kedvesünk okostelefonjára GPS adatokat rögzítő alkalmazást telepíthetünk. Ezáltal folyamatosan tudatában léve annak, hogy merre is jár, illetve nem téved-e rossz ösvényre. Céges információk, mint az ügyfelek névjegyadatai kulcsfontosságú információk, melyek versenytársként megszerezve könnyedén előnyünkre fordíthatunk. Eltulajdonított készülékek esetén, bejelentkezve maradt banki programok által pénzt utalhatunk, online vásárolhatunk vagy az NFC szabvány segítségével kártyás fizetést bonyolíthatunk. Emelt díjas SMS, illetve telefon szolgáltatásra nyílik lehetőség. Valamint fényképeink, videóink, személyes adataink a világhálón köthetnek ki, mely egy, a közzsférában dolgozó személyre rossz fényt vethetnek.

4. ADATGYŰJTÉSI VESZÉLYEK

Az adatgyűjtés kulcsfontosságú szerepet tölt be, mivel nem csak a távközlési terület cégei érdekeltek az okostelefonra való alkalmazások fejlesztésében. Az Internet, majd később az okostelefónia megjelenésével számos új lehetőség nyílt a profitszerzésre. Ezen technikák rohamos ütemben fejlődnek. Nincs idő és kapacitás mindenre kiterjedő biztonsági, élettani, gazdasági vagy éppen társadalmi hatásaikat vizsgálni. (Pintér 2011b) Ezen kis biztonsági rések kihasználásával az illetéktelenek könnyedén hozzájuthatnak kulcsfontosságú adatainkhoz.

A Search Security (Westernvel 2011) kutatásának segítségével mutatom be a top 5 mobiltelefon fenyegetettségét 2012-ben, amellyel személyes információink könnyen hozzáférhetővé válnak.

4.1 Geolokáció alapú támadás

A GPS pozícióink adatai azok közé az érzékeny információk közé tartoznak, melyet nem szívesen osztunk meg a külvilággal. Rengeteg tényadat tudható meg a felhasználóról tartózkodási helye alapján, amit majd kutatásom során egy későbbi fejezetben ismertetek. Kivétel nélkül az összes mobil operációs platform és szolgáltató gyűjti és használja az ilyen jellegű információkat. Több országban tudomásul vették a helyzet fontosságát, valamint jogi lépéseket tettek annak érdekében, hogy a nagy informatikai cégek, mint a Google, hogyan kezeljék lokációs adataikat. Andrew Jaquith, a Perimeter E-Security biztonsági szolgáltatásokkal foglalkozó cég műszaki igazgatója, bűncselekménynek titulálta a GPS pozíciókkal történő visszaéléseket. (Search Security 2011)

4.2 Engedélyek problémái

Telefonunkra letöltött alkalmazásokkal gazdagíthatjuk annak tudását. Ki-ké saját ízlésének megfelelően személyre szabhatja készülékét általuk. Nem is gondolnánk, hogy a programok milyen személyes információkhoz férnek hozzá. Ezek eléréséhez a telepítés során adjuk meg a szükséges engedélyeket, amit sokan automatikusan figyelmen kívül hagynak. Tudatosabb használatnál azonban kiszűrhetők lennének az olyan engedélyekkel való visszaélések – mint SMS-eink vagy telefonkönyvünk adatainak felhasználása – amelyek az alkalmazás funkcióihoz nem feltétlenül szükségesek. Természetesen ezáltal megesik, hogy nehéz döntést kell meghoznunk: választanunk kell, hogy a funkcionalitást vagy a biztonságot részesítjük-e előnyben.

4.3 Alkalmazás okozta sebezhetőség

A Google Android operációs rendszer nyílt forráskódú, programokat bárki írhat és publikálhat. Ez azt jelenti, hogy a felhasználók tömérdek mennyiségű forrásból tölthetik le és telepíthetik a szükséges szoftvereket. Ez természetesen a biztonság rovására megy. Patrik Runald a Websence – web szűrőszoftverekkel foglalkozó cég –

felső vezetőjének szavával élve: *“Ez egy nagyon jó lehetőséget nyújt a rossz fiúknak, melyet hiba lenne elszalasztani”* (idézi O'Rourke 2011 saját fordítás).

A másik nagy versenyző az Apple iOS platformja, amely egy fokkal biztonságosabb rendszer. A fejlesztők alkalmazásai több ellenőrzésen, valamint egy felülvizsgálaton mennek keresztül publikálás előtt. A találékony felhasználó azonban kiötlötte a megoldást annak érdekében, hogy a fizetős programokat ismeretlen forrásból beszerezve, ingyenesen telepíthesse: szoftvermódosítással – Jailbreak-kel – kiiktatják az Apple biztonsági rendszerét, mely így nem látja el funkcióját. Ezáltal könnyedén az adathalász bűnözők áldozatává válhatnak.

Valamint mindkét platform alkalmazásainál megfigyelhetőek programozási hibák, melyet a hozzáértő támadó fél könnyedén ki tud használni. Gondolok itt olyanra, mint felesleges hozzáférés szükségessége, titkosítás hiánya, vagy adatszivárgás például felhő alapú szolgáltatásba² történő szinkronizálásnál. A szabad publikálás hibájának tudható be ez a jelenség. Elkerülése érdekében, javasolt olyan alkalmazásokat letölteni, melyek ismert fejlesztő háttérrel rendelkeznek, mint: Rovio Mobile LTD vagy Ubisoft Entertainment.

4.4 Nem biztonságos WIFI használata

Folyamatosan bővül a nyílt WIFI hálózattal rendelkező intézmények listája. Az okostelefon felhasználók nagy része nem rendelkezik mobil Internet kapcsolattal, ezáltal kihasznál minden ingyenes csatlakozási lehetőséget. Ezen kapcsolatok esetén, a behatolók aránylag egyszerű eszközökkel hozzáférhetnek védtelen készülékünkhöz. Web-es előzményeink, leveleink, jelszavaink, illetve érzékeny adataink könnyen áldozatul eshetnek, egy esetleges támadás során. A nap folyamán akár több ilyen jellegű hálózatra is kapcsolódhat az adott felhasználó, ezáltal mozgása is jól szemléltethető. Megtudható általuk kedvenc kávézónk, étkezdénk, de akár repülővel történő utazásaink állomásai is, amennyiben csatlakozunk az ezen helyek által nyújtott nyílt WIFI hálózatra. Az IBM kifejlesztett egy új biztonságos nyílt WIFI szabványt, amely megoldás lehet a visszaélésekkel szemben. Azonban amíg ez széles körben el nem terjed, a szakemberek nem javasolják az ilyen jellegű hálózatra való kapcsolódást.

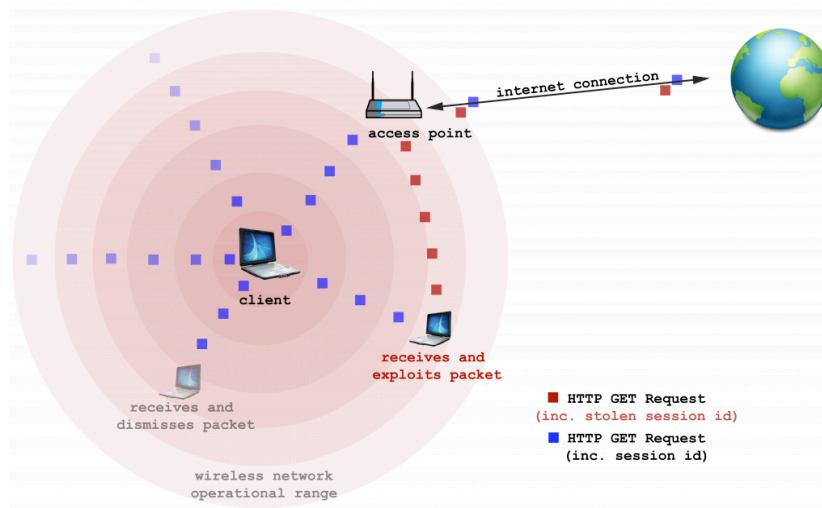
² Hálózati vagy internetes szerveren való adattárolás (Cloud Computing)

A következő fejezetben egy kézzelfogható bemutatóval szeretném szemléltetni a visszaélés könnyedségét, valamint a helyzet súlyosságát.

4.4.1 WIFI hackelés

A WIFI kapcsolat problémáját egy gyakorlati példával fogom szemléltetni. A Droidsheep, német fejlesztésű alkalmazás lesz ebben a segítségemre. Itt jegyezném meg, hogy a szoftver készítői otthoni tesztelésre írták a programot, valamint ezáltal szerették volna bemutatni, hogy mennyire sebezhetőek eszközeink. Semmilyen visszaélési szándék nem vezérelte őket. Természetesen én is csak saját WIFI rendszeremen tettem próbára tudását, valamint a tanulmány befejezése után az alkalmazást töröltem készülékemről.

Miről is van szó tulajdonképpen? Ez egy ARP-Spoof-oló program, mely Androidos rendszeren könnyedén futtatható, amennyiben root³-olt készülékünk van. A lényeg, hogy a támadó beékelődik a WIFI router és a használatban lévő eszköz közé. A kapcsolat innentől fogva a harmadik félen keresztül zajlik, aki ezáltal könnyedén irányítása alá vonhatja a jelfogadó egységet.



Forrás: Droidsheep

Ezáltal az összes olyan munkamenetbe belenézhet, melynél nem a biztonságos http információátviteli protokollt jelölő https sémát használjuk.

³ Root definíció: Alapesetben csak korlátozott felhasználói jogokkal rendelkezünk telefonunk operációs rendszerében. Ezek megszüntetését és ezáltal rendszergazda jogokkal való privilegizált irányítást tesz lehetővé a telefon root-olása. Számos előnye van, mint a telefon teljesítményének növelése, biztonsági másolat készítése vagy védelem kialakítása.

A gyakorlatban a következőképpen néz ki a támadás. A fejlesztő honlapján csak leírások találhatók, maga a program rövid Interneten történő keresés eredményeként lelhető fel. A szoftver telepítéskor csupán három darab engedélyt kér. Teljes Internet hozzáférést, a telefon alvásának megakadályozását, valamint a WIFI állapotának megtekintését. Továbbá indításkor figyelmeztet, hogy semmilyen felelősség nem terheli a készítőt, valamint mindennemű illegális visszaéléstől óva intenek. Ezután a WIFI kapcsolat megléte mellett egy egyszerű start gombra való kattintással elkezdni keresni a mozgásban lévő adatsomagokat. Jelen esetben, hogy szemléltetni tudjam hat darab honlapot töltöttem be melyet hiba nélkül meg is talált. Ezeket az alábbi képen ábrázolom.



Forrás: Saját készítés

A Facebook adatlapom betöltése https használatával történt, így annak tartalmához nem tudtam hozzáférni. Azonban Youtube csatornám és Indamail fiókom kiszolgáltatottá vált. A Droidsheep programon keresztül képes voltam megtekinteni a beállításokat, módosítani tudtam azokat, illetve hozzáfértem mindenféle ezekhez tartozó személyes információhoz. A további általam látogatott – bejelentkezést nem igénylő – honlapok is felderítésre kerültek, ezáltal egy könnyedén visszakereshető, elemezhető előzménylistát hozva létre.

Kerüljük tehát a nyílt WIFI hálózatokat, azonban ha mégis használnunk kell azokat, lehetőség szerint levelezésünket, online rendelés vagy banki tranzakciók lebonyolítását ne ezeken keresztül intézzük.

A lehetséges védelmi eszközöket, dolgozatom egy későbbi fejezetében ismertetem.

4.5 Eltulajdonított vagy elvesztett készülékek

Végül, de nem utolsó sorban, ezt sem lehet figyelmen kívül hagyni. A legtöbbször nem a telefon pótolhatatlan, hanem a rajta tárolt információk. A visszaélés ellen legtöbbször PIN kódot vagy képernyőzárat használnak, azonban készülékünk adatai könnyen kinyerhetők számítógépre való csatlakozás útján. Célszerűbb, a telefon távolról való vezérlése vagy letiltása, de ehhez bizonyos alkalmazások megléte szükségeltetik. Ilyen jellegű szoftverek egyike a Prey, melyet magam is használok. Nem kell mást tenni, mint telepíteni a programot és regisztrálni honlapjukon. Az alkalmazás rejtett módban, tárolódik készülékünkön, ezáltal illetéktelenek nem figyelnek fel rá. A készülék eltűnésekor – ha az bekapcsolt állapotban van és Internet kapcsolattal rendelkezik – igény szerint GPS pozíciót, előlapi kameraképet küld a kétségbeesett tulajdonosnak.

5. KÜLÖNBÖZŐ PLATFORMOK ÉS MOBILSZOLGÁLTATÓK ADATGYŰJTÉSI ELJÁRÁSAI

2011 áprilisában nagy port kavart a hír, hogy az Apple – majd, mint ahogy az később kiderült, az Android is – engedély nélkül adatokat gyűjt és figyel felhasználat. A nyilvánosságra került információk alapján, mindkét platform bizonyos időközönként eltárolja az ügyfél GPS pozícióját, ezáltal rendelkezésre állnak a helyváltoztatásának folyamatos adatai. A témával foglalkozó Guardian cikkében megtalálható (Arthur 2011), hogy a Google készüléke az utolsó kétszáz elérhető WIFI hálózatot és ötven mobilátjátszó-torony helyét rögzíti. Ezek a legrégebbi adattól kezdve folyamatosan felülíródnak. Ezzel szemben az Apple készüléke egy évig tárolja a tulajdonos mozgását rögzítő minden információt.

Az adatok elérésében is különbség mutatkozik. Míg a Google tárolt információi csak a megfelelő informatikai tudással nyerhetők ki, addig az Apple-é könnyedén, közvetlenül a telefonból vagy számítógépből elérhetők.

Ezen felbuzdulva két biztonsági kutató – Alasdair Allan és Pete Warden – készítettek egy bárki számára ingyenesen elérhető számítógépes alkalmazást (Allan – Warden 2011). A felhasználónak nem kell mást tennie, csak szinkronizálnia iPhone vagy iPad eszközét számítógépén. Ezután a program felkeresi a rejtett fájlt – mely a lokalizációs adatokat tárolja –, majd egy térképen szemlélteti az ügyfél mozgását.

Az Apple bejelentéséből kiderült, hogy nem tudtak a fennálló problémáról és azt minél hamarabb javítani fogják a következő iOS verzióban (Houston 2011). Ez meg is történt, azonban sokakban felmerül a kérdés, hogy csak titkosították, elérhetetlenné tették, de továbbra is gyűjtik az adatokat, avagy betartják ígéretüket és felhagynak az ilyen jellegű tevékenységgel.

Természetesen a Google is reagált. Azzal védték magukat, hogy a felhasználók maguk dönthetnek azáltal, hogy a telefon aktiválásakor elfogadják-e a névtelen adatgyűjtést, egy jobb mobil élmény érdekében. Ez esetben az összes lokációs adat küldése a Google szervereire történik, kinyomozhatatlanul és anonim módon. A biztonságot részesítik előnyben és nem adják ki harmadik félnek az adatokat.

Mobilszolgáltatónk szintén felhasználói adatokat tárol, természetesen megőrzési politikájuk sokkal megbízhatóbb. Jogszabály rendelkezik arról, hogy mit gyűjthetnek valamint, hogy az így kapott információkat mennyi ideig kell őrizhetik meg. Mint Magyarország egyik vezető telekommunikációs vállalatának dolgozója, illetékeseket kérdeztem a témával kapcsolatban. Kollégáim elmondták, hogy az adatgyűjtés kizárólag a számlázás érdekében történik. Csak a rendőrség számára adhatók ki személyes adatok, amennyiben arra írásos formában hivatalos kérvény érkezik. Bármilyen információ harmadik félnek való kiadása büntetőjogi eljárást von maga után. A mobilszolgáltatók adatgyűjtéssel kapcsolatban a következő tényadatok tudhatók:

- Gyűjtik a bejövő és kimenő híváslistát. Kit hívott az ügyfél, vagy kitől fogadott hívást, illetve a beszélgetés időtartama kerül listázásra.
- Kinek küldött, illetve kitől kapott SMS üzenetet.
- Milyen gyakran kapcsolódott Internetre és mekkora adatforgalmat generált.

- Valamint természetesen a lokalizációs adatai kerülnek feldolgozásra cellainformációk segítségével.

A hozzáférés cégen belül csak bizonyos személyek számára engedélyezett. Nekik különböző titoktartási szerződéseket kell aláírniuk, amelyben biztosítják az információk bizalmas módon való kezelését. Fejlesztő és tesztelő munkatársak pedig nem a valós, hanem fiktív adatokkal dolgoznak, ezzel mindennemű visszaélést lehetetlenné téve.

A gyűjtések ellen a felhasználó nem tehet semmit. Akit a téma ennél mélyebb szinten is érdekel, annak érdemes felvenni a kapcsolatot a mobilszolgáltatóval, vagy megkeresni annak adatvédelmi irányelveit online.

Tény, hogy az ilyen jellegű adatokra a szolgáltatóknak szüksége van, mivel jóval nagyobb felhasználói élményt tudnak nyújtani ezen információk elemzése által. Legfontosabbak a geolokációs adatok. Felhasználásuk nagy előrelépés különböző fejlesztések folyamán. Operációs rendszerek esetén, gondolok itt például a térképszolgáltatásokra. Mobilszolgáltatók esetén, a még lefedetlen területek feltérképezésére vagy mobil átjátszó tornyok kapacitásának meghatározására. Addig nincs is ezzel probléma, amíg ezek biztonságban tárolódnak. Azonban, amint ez illetéktelen kezekbe jut, következményei felbecsülhetetlenek.

6. FOGYASZTÓI ÉRDEKVÉDELMI SZERVEZETEK ÉS MUNKÁSSÁGUK

Köztudott, hogy számtalan fogyasztói érdekvédelmi szervezet működik világszerte, munkásságukról azonban viszonylag keveset tudunk. Jelen fejezetben a legnagyobbak közül szemléltetnék párat.

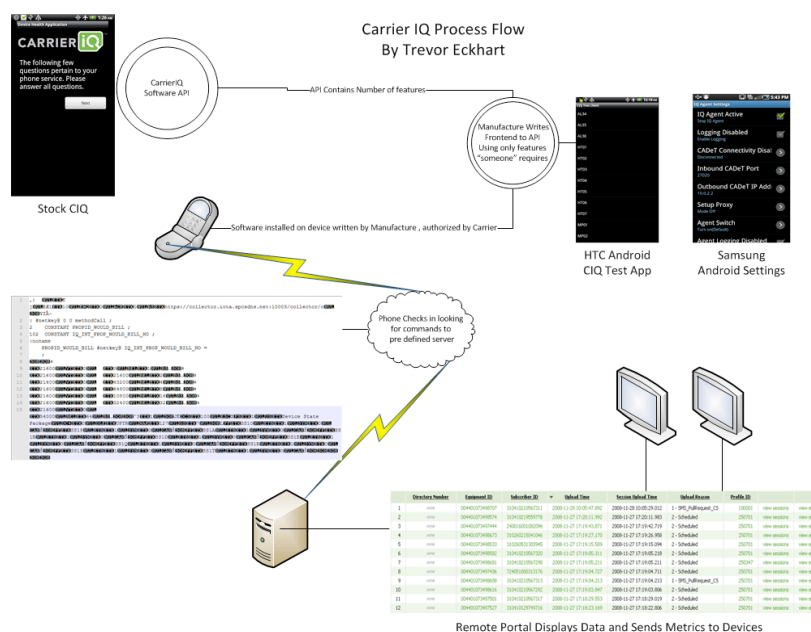
6.1 Electronic Frontier Foundation

Az Apple és a Google adatgyűjtési aggodalma mellett egy másik nagy hír is megmozgatta a világ IT szakembereit 2011-ben. Főként az USA szolgáltatói által az okostelefonokra – hibakeresésre és minőségjavításra – feltelepített Carrier IQ program, az egyik legnagyobb adatgyűjtő botrányba keveredett. Először Android rendszeren majd az Apple termékein is világszerte felfedezhető volt kémkedő tevékenysége.

Egy biztonsági szakértő, bizonyos Trevor Eckhart észlelte a rejtett szoftver létezését és kártékony hatásait. Kutatni kezdett, majd közzétett egy részletes leírást, mely a program illegális működéséről szólt (Eckhart 2011a). Állításait tényadatokkal bizonyította, valamint rootkit⁴-ként titulálta az alkalmazást. A hír hallatán a CarrierIQ feljelentést tett és nyilvános bocsánatkérést követelt. (Shankland 2011) Trevor nem hagyta annyiban és ekkor fordult segítségért egy civil Internetes jogvédő szervezethez az Electronic Frontier Foundation-hez (EFF). Ekkor már nagyobb lapok is – mint a Wall Street Journal vagy a New York Times – érdeklődést mutattak a hír hallatán. A CarrierIQ próbálta menteni a menthetőt: félreértésre hivatkozva bocsánatot kért, de innen már nem volt visszaút.

Trevor egy újabb bejegyzésben szemléltette – amely már videót is tartalmazott – a program illegális mivoltát (Eckhart 2011b). Több fórumon felmerült, hogy esetleg az FBI állhat a háttérben, azonban ezen információk bizonyítására eddig nem került sor.

A program telefonok tevékenységeinek nagy részét monitorozza, majd a kapott adatokat a szervernek továbbítja a készülék egyéni azonosítójával együtt.



Forrás: Trevor 2011b

A létrejött adathalmazból könnyedén visszakereshetők SMS-eink, email-jeink, telefonhívásaink, billentyű leütéseink, GPS koordinátánk és még rengeteg személyes

⁴ Rootkit definíció: Kártékony szoftver, amely rejtett hozzáférés segítségével bizalmas adatokat szerez a fertőzött készülékről. (VírusHíradó 2012)

információnk. Az adatgyűjtés ténye vitathatatlan, azonban visszaélésről nincs információ.

Az EFF végül elérte, hogy a CarrierIQ bocsánatot kérjen, továbbá hogy alkalmazzon egy a szakmájában nagy elismerésnek örvendő biztonsági szakembert Magnolia Mobley-t (Bohn 2012). Ígéretet tettek, hogy a cég a jövőben jóval nagyobb figyelmet szentel a felhasználói adatok biztonságos tárolásának és felhasználásának.

A felhasználó azonban továbbra sem dőlhet hátra és érezheti magát teljes biztonságban. Ezt igazolják a WikiLeaks főszerkesztőjeként ismert Julian Assange londoni előadásán elhangzott tényadatok, miszerint 25 országban több mint 150 CarrierIQ-hoz hasonló szervezet van, ami mobil megfigyelésre szakosodott. (Haselton 2011) Úgy vélem ez kellő ok az aggodalomra.

6.2 Federal Trade Commission

Másik nagy élen járó szervezet a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission). Tevékenységei közé sorolandó a személyes információk Internetes kezelésének szabályozása, illetve nagy cégek – mint a Facebook – adat-felhasználási módszereinek szankcionálása.

Az FTC folyamatos kampánya kimondja, hogy a cégeknek be kell tartani biztonsági ígéreteiket, melyeket a felhasználóknak tesznek. (Federal Trade Commission 2012a) Ennek érdekében jogi intézkedéseket eszközöl és nem riad vissza vezető óriáscégek megbüntetésétől sem (2012 szeptemberében a Google-el 22,5 millió dolláros bírságban egyeztek meg, mivel a keresőcég kihasználta az Apple Safari böngészőjének biztonsági réseit és ezáltal adatokat gyűjtött a gyanútlan felhasználókról). Jon Leibowitz az FTC elnökének szavával élve *“A mérettől eltekintve, minden vállalatnak ragaszkodni kell az FTC által hozott rendeletekhez...”* (Federal Trade Commission 2012b saját fordítás). Kampányuk nagy elismerést és támogatást vált ki a felhasználók, valamint a vállalatok körében is.

Az FTC másik kampánya a gyermekek személyiségi jogainak védelmére irányul (Federal Trade Commission 2012c) Több okostelefon alkalmazásnál is felmerült a probléma, hogy azok nem megfelelően járnak el az adatok védelmével kapcsolatban. Harmadik félnek szolgáltatják ki a megszerzett információt, így például személyre szabott reklámokkal tudják bombázni a felhasználót. Ezzel még nem is lenne

probléma, azonban az FTC által vizsgált játékok között olyanokat is találtak, amelyek valódi pénz elköltésére ösztönözték a gyerekeket (Sperry 2012). Az okostelefonok felhasználói adatainak kinyerése által, meghatározható az ügyfél életkora, ezáltal kihasználhatóvá válik a kiskorúak naivitása. Ennek érdekében a szervezet új szabványok létrehozását tervezi, melyek nagyobb biztonságot nyújtanak, illetve lehetővé tennék a szülők számára az adatok áramlásának bizonyos fokú kontrollálását. A gyors cselekvés szükségessége vitathatatlan. A fiatalok egyre korábban kezdik el használni ez Internetet, valamint egyre több, kifejezetten gyermekek számára készült alkalmazás lát napvilágot. A problémák elkerülése érdekében, már a programozás fázisában meg kell szabni a szükséges előírásokat, valamint teret kellene engedni a szülői kontroll lehetőségének. Megoldás lehet a problémára, egy alkalmazás, mely a kiskorúak készülékére történő telepítés után minden esetben értesíti a szülőt, és engedélyt kér mielőtt a gyermek alkalmazást telepítene, illetve azon belül pénzt költene.

6.3 Aktualitás

2013 tavaszán a Google újabb hibás adatkezelési botrányától hangos a sajtó. Egy ausztrál fejlesztő saját blogján tette közzé felfedezését. Megtudhatjuk belőle, hogy aki a Google Play áruházban vásárolt terméket, annak személyes adatai – mint név, email cím és város szintű lokalizáció – elküldésre kerülnek az aktuális fejlesztőnek. (Nolan 2013) Ez önmagában nem is okozna problémát, mivel a felhasználó adja meg ezeket az információkat, azonban nem járul hozzá ezek harmadik félnek való kiadásához.

Utánajárva a témának kiderült, hogy azt a személyt, aki alkalmazásait pénzért árulja a Play áruházban adózási kötelezettség terheli, melynek jogi teendőit önmagának kellene elintéznie. Ehhez szüksége van az adott vásárló lakhelyére, azonban a többi – a Google által kiadott – adat hozzáférhetőségének okai tisztázatlanok. (Az Apple-nél ez nem fordulhat elő, mivel ott a cég végzi el a szükséges jogi lépéseket.) Még egyik nagy érdekvédelmi szervezet sem támogatja az ügyet, azonban ami késik, nem múlik. Jelenleg itt tart az eljárás, kíváncsian várjuk a fejleményeket.

7. ALKALMAZÁSOK

A Google, az Apple és a többi szolgáltató is szoftverek százazeit ajánlja a felhasználóinak, készülékük tudásának kibővítése céljából. Mindenki megtalálja az igényeinek megfelelő applikációkat. Van, amelyikért fizetni kell, de rengeteg ingyenes is fellelhető ezeken az online piactereken.

7.1 Mi alapján döntünk?

Szoftverválasztásunk folyamán döntésünket legfőképpen anyagi kereteink befolyásolhatják, azonban ingyenes alkalmazások közül is számtalan áll a felhasználó rendelkezésére. Szűkítve ezáltal a kört, a következő döntést támogató tényezők lehetnek, embertársaink felhasználói értékelései. Véleményüket kinyilváníthatják 1-5 csillagos pontozással valamint szöveges minősítéssel. TDK kutatásom során, megdöbbenve tapasztaltam, hogy ezeket is befolyásolják a nagy programozó cégek. Az okostelefon alkalmazásokra nagy a kereslet, ezáltal az igények kielégítésére hatalmas kínálat alakult ki. Az új piac kiaknázására több cég is felfigyelt. Mivel rengeteg a hasonló profilú szoftver, a vállalatok megtévesztő, saját maguk által kreált hamis értékelésekkel próbálnak kitűnni a tömegből. Feltornászva ezáltal a program letöltési darabszámát, nagy pénzbevételhez juthatnak.

7.2 Ha nem pénzt, akkor mit adunk cserébe?

Ne tévesszen meg bennünket a látszat, hogy ingyen jutunk hozzá modern alkalmazásokhoz, mint zenefelismerő, vagy navigációs program és cserébe nem kell semmit sem nyújtanunk. Valamilyen formában minden szolgáltatásért adnunk kell valamit, vagy el kell viselnünk az ingyenességből adódó hibáit, hiányosságait. Ezért is fontos a gyermekek felhasználói szokásaira nagyobb odafigyelést fordítani, mivel ők sokkal hiszékenyebbek, mint felnőtt embertársaik. Könnyebben dőlnek be marketingfogásoknak és egyszerűbb őket megvezetni, ezáltal akár anyagi károkozás áldozatává is válhatnak. Lássuk mi az a tipikus három dolog, amivel együtt kell élnünk, ha az ingyenességet választjuk. (Természetesen ezek kombinációi a legelterjedtebbek, de könnyebb megértésük érdekében külön taglalva mutatom be őket.)

7.2.1 Hirdetések

A legtöbb ingyenes alkalmazás rendelkezik hirdetői felülettel. Nem feltétlen zavaró, ámde folyton jelenlévő reklámokról beszélünk. A fejlesztő ezek után kapja a pénzt, ezért az ingyenesség, hogy minél több emberhez eljusson. Amennyiben a készítő minimális adatgyűjtéssel – mint geolokációs pozíció – egészíti ki szoftverét, személyre szabott hirdetések juttathatók el a felhasználók felé. Természetesen ez versenyelőnyt jelent, valamint ebből kifolyólag több pénzt kérhet el a beágyazott reklámokért, illetve keresettebb lesz a hirdetők szemszögéből. Több esetben a szoftver fejlesztője felajánlja a reklámmentes verzió megvásárlásának lehetőségét. Így mindkét fél elégedett lehet, a fejlesztő pénzhez jutott, a felhasználó pedig reklámok nélkül élvezheti az applikációt.

7.2.2 Demó verziók

Létezik olyan, hogy egy alkalmazás fizetős és ingyenes változatban is jelen van az adott piacon. Ezáltal egy ingyenes demó verzió segítségével kipróbálhatja a felhasználó és dönthet arról, hogy érdemes-e azt megvásárolnia. Természetesen ez nem rendelkezik az összes létező funkcióval, valamint használatának akár időkorlátja is lehet. Viszont amennyiben a fogyasztó megkedveli pozitív adottságait, szívesen fizet annak érdekében, hogy a továbbiakban is használhassa az adott szoftvert készülékén.

7.2.3 Alkalmazáson belüli vásárlás lehetősége

Még csak gyermekcipőben jár, azonban egy nagy lehetőség az alkalmazáson belüli vásárlás. Főként játékoknál használják, ahol különböző extrák eléréséhez valódi pénzt kell költenünk. A legelterjedtebb a kredites rendszer, amikor is egy adott összeg kifizetése után, adott mennyiségű kredittel rendelkezik a felhasználó. Ez különböző dolgokra használható fel a játék folyamán. Természetesen hamar elfogy és a szoftver újabb pénzköltésre ösztönöz. Itt jön szóba a gyermekek védelme. A kiskorúak legfőképpen játékokat használnak készülékükön. A szülők tudta nélkül költhetnek el nagyobb pénzösszeget, mely csak a számla megérkezésekor jelentkezik. A szülőknek meg kell adni a lehetőséget, hogy ezt kontrollálni tudják. Ennek érdekében tesz nagy erőfeszítéseket világszerte több fogyasztói érdekvédelmi szervezet.

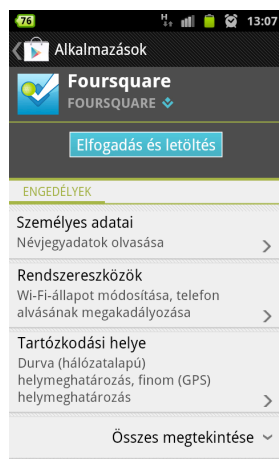
Jelenleg PIN kód megadása szükségeltetik, az online boltokban történő vásárlás lebonyolításához. 2013 tavaszán azonban sikerült egy öt éves gyermeknek 1700 fontot elköltenie a Zombies vs. Ninjas játék kiegészítőire édesapja Apple Ipad-ján. (Philips

2013) Az ingyenes alkalmazás telepítéséhez szülei megadták a szükséges PIN kódot. Azonban annak nem voltak tudatában, hogy a felhasználó, a jelszó megadása után 15 percig szabadon költhet bármire. Gyermeük fel sem fogta, hogy a család vagyonát csökkenti, így belement a játékot segítő kiegészítők vásárlásába. A szülők nagy meglepetését váltotta ki a másnap érkező banki kimutatás. Amint realizálták a probléma eredetét, rögtön az Apple-höz fordultak és kártérítést követeltek. A nagy szolgáltató eleinte nem akarta visszafizetni a jelentős összeget, azonban végül engedett és megtérítette a teljes költséget.

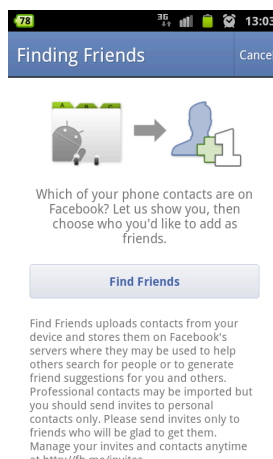
7.3 Programok névjegyzék gyűjtése

Akár fizetős akár ingyenes alkalmazásról is beszélünk, a visszaélések mindennapos gyakorlatáról van szó. Több alkalmazás hozzáfér a telefonon tárolt névjegyzékeinkhez, amelyet én az egyik legszemélyesebb adatok egyikének gondolok. Saját szervereiken gyűjtik, tárolják az információkat. Harmadik félnek való kiadásuk egyenlőre ismeretlen. Ilyen alkalmazás a Facebook, Foursquare, Twitter, Gowalla vagy Instagram, amelyek ezáltal elküldik a kontaktok telefonszámait, email címeit egy központi gépnek. Ennek segítségével egyezéseket keresnek, így ismerősöket tudnak ajánlani az ügyfeleknek ezzel is gazdagítva a felhasználói élményt. A probléma ott kezdődik, mikor saját profitszerzésük érdekében használják föl az így összegyűjtött információkat.

Android platformon már elterjedté vált, hogy a telepítéskor az engedélyek között megjelenítik a névjegyadatok gyűjtését, vagy az alkalmazás adott funkciójának használata előtt tüntetik fel az ezzel járó hozzáférés szükségességét.

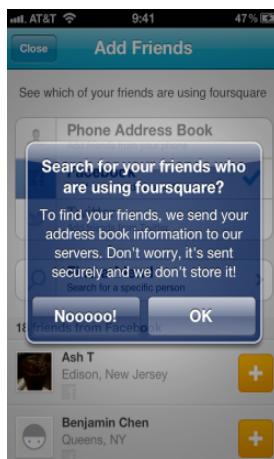


Forrás: Saját készítés



Forrás: Saját készítés

Az Apple szoftverei telepítéskor nem kérnek engedélyeket, azokat az alkalmazás használata közben – a szükséges funkcióhoz tartozó oldalon – egy felugró ablakban lehetséges engedélyezni.



Forrás: Van Grove 2012

Azok a fejlesztők akiknek a programjai engedély nélkül adatokat gyűjtenek, büntetésben valamint az online áruházból való kitiltásban részesülnek az Apple irányelveinek megszegéséért.

Több olyan szoftver is átjutott már az Apple biztonsági rendszerén, mely a felhasználó jóváhagyása nélkül gyűjtött adatokat. Amíg egy lelkes hozzáértő fel nem fedezi, addig azok több kárt, mint hasznot eredményeznek. Az egyik legjobb példa erre a Facebook kihívójának is nevezett Path közösségi program. Arun Thampi, egy szingapúri programozó figyelt fel az engedély nélküli névjegyadatok másolására. Blogbejegyzésben közhírré is tette felfedezését, melyre a Path vezetősége rövid időn belül válaszolt. David Morin vezérigazgató „*Legjobb ipari gyakorlat*” -ként titulálta a vádakat. (Bilton 2012 saját fordítás) A gyakorlatban fellelhető különbség, hogy más versenytárs engedélyt kér az adatok gyűjtéséért és nem a felhasználó tudta nélkül teszi azt. Emellett a Path szerverein tárolt információk bárki által hozzáférhetőek voltak, mivel a cég semmilyen titkosítást nem alkalmazott, ennek elkerülése érdekében. A nagy felháborodás eredményeképpen a vállalat ígéretet tett arra, hogy az eddig összegyűjtött adatbázisokat megsemmisíti és felhagy a telefonkönyvek tartalmának gyűjtésével.

7.4 Engedélyek kijátszhatósága

Ebben a fejezetben a ViaForensics – biztonsági szoftvereket gyártó cég – demonstrációját mutatom be. (Cannon 2011) Tartalma egy a cég által kísérleti célra elkészített Android alkalmazás, mellyel Internet kapcsolat megléte mellett átvehető telefonunk teljes irányítása. Egy egyszerű játékkal csalják törbe az áldozatot. A program telepítéskor nem kér semmilyen engedélyt, ezáltal a felhasználó megnyugszik, hogy egy teljes mértékben biztonságos szoftvert használ készülékén. Azonban a játék elindítása után, az a háttérben elkezd monitorozó tevékenységét, mely az alkalmazásból való kilépés után sem szűnik meg. Az Internet segítségével csatlakozik a távoli támadó félhez. Ennek kivitelezését az Android beépített böngészője segítségével oldja meg, mivel az rendelkezik az Internet eléréséhez szükséges engedélyekkel. Ezáltal a készülékünkön tárolt képeink, jelszavaink, böngészési előzményeink, jelenlegi pozíciónk, névjegyzékünk adatai, egyszóval mindenfajta érzékeny információnk a támadó fél tulajdonába kerül. A demonstráció jól mutatja, hogy az Android előnyei, mint erő és rugalmasság, hátrányként is könnyedén feltűntethetőek. Azonban a tervező elmondása szerint, bármilyen platformon hasonlóképpen kivitelezhető ez a fajta visszaélési mód.

7.5 Alkalmazások összehasonlítása

Ebben a fejezetben górcső alá veszek tíz darab Android navigációs alkalmazást – név szerint: CoPilot, Egérút, Google Maps, Navigon, Navitel, NDrive, Route66, Sygic, TomTom, Waze – és biztonsági szempontból vizsgálom őket. A felhasználók által, legjobbnak ítélt programok közül szemezgettem, ezáltal hét darab ingyenes és három darab fizetős került összehasonlításra. Nem a programok tudására, vagy precizitására voltam kíváncsi, hanem hogy milyen engedélyeket kell a felhasználónak elfogadnia futtatásuk során.

Mint azt már korábban is említettem, Android platformon a szükséges engedélyek listáját jóvá kell hagynunk telepítés előtt. Már itt megállnék egy pillanatra. Három féle csoportba sorolnám ezt a listát. Első, amik a telefonkészüléken rögtön láthatók, olvashatók. Második, amelyek az “Összes megjelenítése” fül lenyitása után érhetőek el. Harmadik csoportba pedig azokat sorolnám, melyek csak a böngésző által lelhetők fel.



Forrás: Saját készítés

A pozitívumok közé tartozik, hogy a Google magyarázattal is szolgál az engedélyek mivoltával kapcsolatban – mint az a képen is jól látható. Azonban nem tartom korrekt megoldásnak, hogy a híváslista olvasás és módosítás engedélyének szükségessége kizárólag számítógépről érhető el. Ezek rövid leírásában megtaláljuk, hogy az alkalmazás a bejövő és kimenő híváslistánkat olvashatja, illetve van olyan, ami módosíthatja is. Valamint feltüntetik, hogy a lementett névjegyzékünk adatait kártékony programok a tudtunk nélkül harmadik féllel oszthatják meg. Tíz általam vizsgált alkalmazás közül hét darab olvashatja és kettő módosíthatja is a híváslistánkat, köztük a Google gyárilag telepített – ezáltal csak speciális módon törölhető – Google Maps szoftvere.

A meglepetések ezzel azonban nem értek véget. Felkeltették figyelmemet a díjköteles szolgáltatások engedélyének szükségességei is. Tízből öt darabnál kell engedélyezni telefonszámok közvetlen hívását, három darabnál pedig SMS üzenet küldését. A Google felhívja a figyelmünket, hogy ez költséget eredményezhet, illetve, hogy visszaélés áldozatává válhatunk. Ezen a ponton vettem észre, hogy a magyar fordítás teljesen más információt közöl a “Telefonszámok közvetlen hívása” engedély magyarázatával kapcsolatban, mint a honlapon fellelhető angol szöveg. Magyarul így hangzik: “Lehetővé teszi az alkalmazás számára az Internetes geolokációs engedélyek módosítását. Engedélyezése esetén rosszindulatú alkalmazások helyadatokat küldhetnek tetszőleges webhelyre”. Nem mindegy, hogy az alkalmazás telefonál és

SMS-t küld vagy helyadatokat közöl. Valószínűleg fordításból eredő probléma van a háttérben, de ez nagymértékben megtéveszti a felhasználót. Valamint utánajárván, különböző fórumokban megtaláltam a telefonhívás, illetve SMS küldés miértjének okát. A Google Maps esetében arra utal, hogy különböző cégek, boltok találhatóak az adatbázisban címmel, telefonszámmal, melyet a programon keresztül egyszerűen és könnyedén tudunk tárcsázni. Ez a többi navigáció esetén is hasonlóképp működik. Azonban a visszaéléssel kapcsolatos figyelmeztetés nem megnyugtató.

Amint azt már korábban is említettem több alkalmazás hozzáfér névjegyzékünk adataihoz. Jelen esetben tízből nyolcnál tapasztaltam ezt a fajta engedélykérést. További érdekesség, hogy négy program fényképezésre, videó illetve hang rögzítésére is képes. Természetesen erre is van magyarázat. A hang alapú vezérlés feltétele a hangrögzítés. Illetve kameránk segítségével például monitorozhatjuk az előttünk haladó gépjármű rendszámát, ezáltal könnyebbé téve a lopott autók felderítését hazánkban. Az adatgyűjtés ezen pozitív oldalát majd egy későbbi fejezetben ismertetem.

Csupán egy szoftver akart névjegyadatokat módosítani, kettő darab pedig naplófájlokat olvasni. Szintén két darab kért engedélyt a futó alkalmazások lekérésére és közülük csak az egyik akarta azokat be is zárni. Adatokat fogadni három darab szeretne az Internetről. Ezek legfőképpen forgalmi információk, melyek alternatív utak kiválasztásával a gyorsabb közlekedést teszik lehetővé. A Google Maps mellett pedig csak egy akart automatikusan elindulni bejelentkezéskor.

Furcsának találtam viszont, hogy a Google Maps-on kívül egyik sem kért engedélyt parancsikon telepítésére, márpedig ez a funkció mindegyikben megvan és telepítéskor automatikusan életbe is lép. A másik, hogy az Egérút nevű alkalmazás csupán négy darab engedélyt kért, míg versenytársai kivétel nélkül tíz feletti engedélynek a meglétét szerették volna magukénak tudni. Két lehetőség merül fel ezzel kapcsolatban. Vagy az Egérút nem tüntet fel minden lehetséges opciót, vagy négy darab engedély is elég egy teljes értékű navigáció futtatásához, ezáltal a többire nem feltétlenül van szükség. Feltelepítve és még jobban megvizsgálva pár alkalmazást azt tapasztaltam, hogy ugyan négy engedély megléte nem elég viszont tíz alatti számokról kellene beszélnünk. A legfontosabbak, melyek szükségesek egy jól működő, modern és extrákkal felszerelt navigációs szoftver futtatásához a következők: durva hálózat alapú, illetve precíz GPS alapú helymeghatározás, teljes Internet hozzáférés, telefon alvásának

megakadályozása, billentyűzár letiltása, telefon állapotának olvasása, adatok fogadása az Internetről, valamint a parancsikon telepítése.

A másik érdekesség, hogy habár a Google engedélyek kérésére kötelezi a fejlesztőket, szinte mindegyiknél feltünteti, hogy engedélyezése esetén rosszindulatú alkalmazások áldozatává válhatunk. Így bújva ki az esetleges jogviták alól, továbbá a felelősség innentől fogva teljes mértékben az ügyfelet terheli. Itt kezd el gondolkodni a tudatos felhasználó: Hogy is van ez? Az engedélyeknek egyfajta kontroll szerepet kellene ellátniuk a visszaélések és adataink kiszivárgásának elkerülése érdekében. A gyakorlatban – mint ahogy azt összehasonlításom is jól mutatja – ez nem egy zökkenőmentesen működő dolog. Azonban akkor mi értelme is van az engedélyek kérésének. Mi az, amit nyugodt szívvel telepíthetek?

Egyenlőre ezek a kérdések megválaszolatlanok, azonban reméljük a jövő változást hoz e tekintetben. Addig is próbáljuk meg ismert fejlesztők termékeit használni és odafigyelni arra, hogy milyen adatokat tárolunk eszközeinken.

7.6 Aktualitás

2013 februárjában látott napvilágot a hír, hogy egy amerikai multinacionális biztonsági cég – a Raytheon – kifejlesztett egy számítógépes programot, mely különböző felhasználói szokásokat figyel a közösségi szájtokon. (Gallagher 2013) Köztudott a tény, hogy az ilyen jellegű alkalmazásokat, mint Facebook, Twitter, Gowalla vagy Foursquare használjuk leggyakrabban okostelefonunkon. Folyamatosan értesülünk a legújabb fejleményekről, valamint rendszeresen osztjuk meg fényképeinket, tartózkodási helyünket vagy aktuális állapotunkat ismerőseinkkel. A Rapid Information Overlay Technology (RIOT) elnevezésű szoftver ezek segítségével gyűjt információkat a felhasználó jövőjének előrejelzése érdekében.

Lássuk mit is tud a program valójában. Különböző helyekre való bejelentkezéseink, valamint telefonunk által készített fényképeink GPS adatai alapján, Google Maps térképen szemlélteti, hogy mikor merre jártunk a nagyvilágban. Ezáltal nem csak mozgásunk, de a képek segítségével kinézetünk is felderítésre kerül. Jövőnk könnyedén jósolható a program által készített statisztikákkal. Elemzi többek közt a tíz leglátogatottabb területet, ahova valószínűleg a közeljövőben vissza fogunk térni. Itt nem áll meg azonban a kutatás. Mélyebbre ásva analizálja a különböző helyeket, majd

diagramok segítségével havi, heti továbbá napi bontásban szemlélteti a bejelentkezések számát. Így még nagyobb – szinte órás – pontossággal jósolható jövőbeni pozíciónk. A szoftver sajátossága többek között, hogy a közösségi szájtokon létrejött kapcsolatainkat is képes mutatni. Ezáltal a felhasználóról a legtöbb lényeges adat a cég tulajdonában van.

Fontos információ, hogy a program jelenleg még nem került értékesítésre, azonban az amerikai kormány már látta és nagy lehetőségeket vélt felfedezni benne. (Gallagher 2013) Kíváncsisággal tölt el a jövőbeni alakulása, felhasználásának területe, valamint a biztonság megoldásának kivitelezése.

8. GEOLOKÁCIÓS KUTATÁS

A Raytheon cég RIOT szoftverének megismerése után kutatási célként tűztem ki, hogy bemutatom mobilkészülékünk geolokációs adatai alapján, milyen információk tudhatók meg a felhasználóról, illetve annak jövőbeli tevékenységeiről. Elképzelésemet továbbá Barabási Albert László fizikus szavai ösztönözték, miszerint *„az emberi mozgás is kutathatóvá, mérhetővé, matematikai és statisztikai szempontból elemezhetővé válik”*. (idézi: Mindentudás 2011). Valamint az Interneten többek által felvetett elméletet szerettem volna megvizsgálni, miszerint az ember jövőbeni tartózkodási helye – bizonyos tényadatok birtokában – 100 méteres körzetben magasabb, mint 90%-os pontossággal megjósolható.

Nem is hinnénk, hogy szimpla GPS koordináták alapján mennyi minden tudható meg a felhasználóról. Gondolok itt olyanra, mint lakhelye, munkahelye, közlekedési szokásai, valamint szabadidős tevékenységei. Ezek olyan személyes információk, melyeket nem szívesen osztunk meg a nagyvilággal pláne, ha ezáltal könnyedén visszaélés áldozatává válhatunk. Szóval érdemes odafigyelni milyen forrásból származó alkalmazásokat telepítünk készülékünkre.

Mint ahogy azt már korábban említettem, nem csak a különböző térkép szoftverek monitorozzák és tárolják a GPS koordináták adatait. Olyanok is, melyek funkcióihoz az nem feltétlen szükséges. Kétféleképpen történhet a lokalizáció: durva hálózat alapú – cellainformációk segítségével – vagy precíz GPS helymeghatározás által. Erre mai olcsóbb kategóriás készülékeink is képesek, azonban nem új keletű

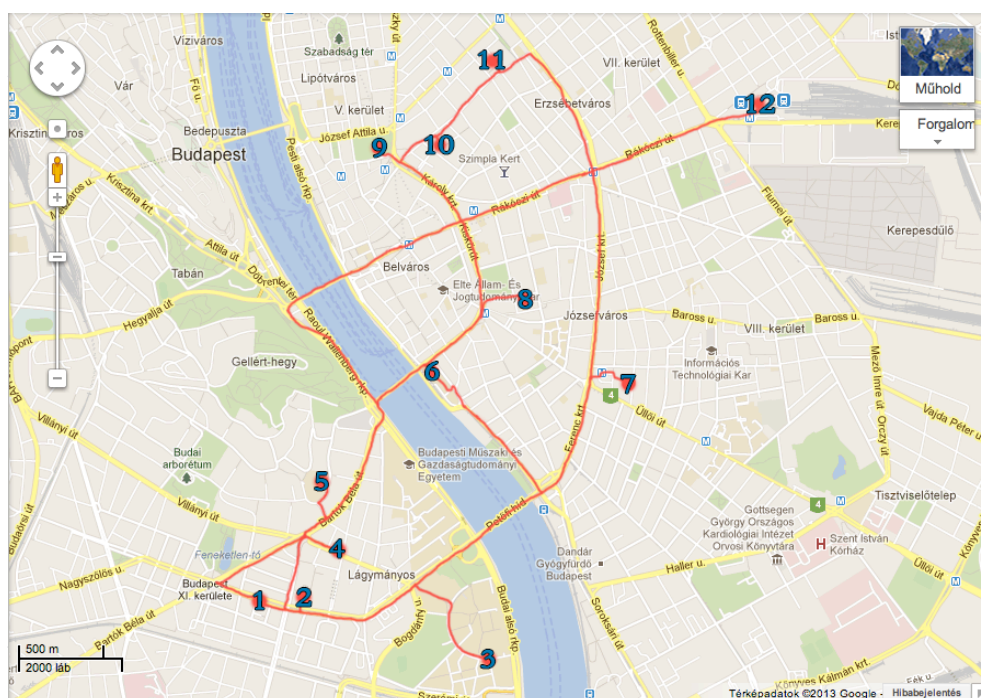
felfedezésről beszélünk. Még az okostelefónia előtti időkben is – cellainformációk segítségével – aránylag nagy pontossággal tudható volt a telefonáló tartózkodási helye.

Saját adataim kutatását adatvédelmi szempontból, nem tartottam biztonságosnak. Ebből kifolyólag anonim módon két ismerősöm egy hetes geolokációs pozíciói kerülnek bemutatásra. Kezdetben különböző alkalmazások által történt az adatgyűjtés. A Google Play áruházából szemezgettem, mivel mindkét telefon Android operációs rendszert futtat. Nagy figyelmet fordítottam arra, hogy megbízható forrásból kerüljenek telepítésre az applikációk. Ezáltal ismert fejlesztők termékeit használtam és elvettem a kétes eredetű szoftvereket. Kipróbálásra került a Nike fejlesztése a Nike+ Running, a legjobbra értékelt RunKeeper, valamint az Adidas üdvöskéje a miCoach. Kellő pontossággal térképezték fel a bejárt útvonalat, azonban futtatásuk sajnos az akkumulátor üzemidő kárára volt.

További kísérletezgetés után, úgy döntöttem, hogy idő és kapacitás hiányában egyszerű módszerhez folyamodom. Arra kértem ismerőseimet, hogy minden este egy Excel táblázatban tüntessék fel az aznap látogatott fontosabb intézmények címei, az ott eltöltött idő intervallumát, valamint jelöljék meg a heti szinten ismétlődő eseményeket. Telefonunk által folyamatosan monitorozott GPS pozíciók alapján ugyanis ezek az alap adatok tudhatók biztosan. Itt jegyezném meg, hogy ismerőseim hozzájárulásukkal szívesen segítettek TDK dolgozatom eme szekciójának elkészültét. Összevetve az így kapott adatokat, a jobb átláthatóság érdekében Google térképeken szemléltetem a megadott helyeket, valamint a köztük bejárt útvonalat.

A munka oroszlánrésze, azonban csak ezután következett, kihívást jelentett a címekhez épületeket kapcsolni. A Google keresője és óriási adatbázissal rendelkező térképe nagy segítséget nyújtott a feladat végrehajtásában. Ezáltal tulajdonomba került az ismerőseim teljes heti menetrendje, szinte percre pontosan.

Kezdjük a férfi ismerősöm által gyűjtött információk kiértékelésével. Térképes formába öntve ezek a következők:



Forrás: Saját készítés

A képen a hétköznapi adatok egyben találhatóak. A kapott adatbázis alapján tizenkettő darab fontosabb helyet jelöltem be rajta, ahol huzamosabb ideig tartózkodott. Kezdjük azok bemutatásával, amelyek heti szinten ismétlődnek. Lakhelye könnyen megállapítható, mivel minden reggel 8 órakor itt lett aktív a GPS jel és este éjfél körül itt került offline állapotba a készülék. Ezt egyes számmal jelöltem. Két olyan hely van ahol a legtöbb időt töltötte. Ezek a hármas és hatos számú pontok. Előbbi következtetni lehet munkahelyére, mely a Magyar Telekom Nyrt. Infoparkban lévő G épülete. Heti húsz órát tölt itt, naponként lebontva hétfőn és csütörtökön nyolcat kedden délután pedig négyet. A hatos számmal jelölt intézmény a Budapest Corvinus Egyetem E épülete, ahol szintén legalább heti tíz órát tartózkodik, órarendje szerint adott időpontban. Hétfőn és szerdán fél nyolctól kilencig rendszeresen látogatott az ötös számmal jelölt hely, ami a Mátyási úti Uszoda. Valamint hétfőn este úszás után a négyes számmal jelölt Pinyó klub ahol az Internetről könnyedén megtudható, hogy ebben az intervallumban QuizNight azaz kocsma kvíz csapatvetélkedő zajlik. Ezen kívül heti többször vásárol a kettes számú Fehérvári úti vásárcsarnokban. Legalább egyszer megfordul a nyolcas számmal jelölt Fővárosi Szabó Ervin könyvtárban, valamint egy plázában. Jelen esetben a Corvin bevásárlóközpont szerepel a heti listáján hetes számmal jelölve, illetve legalább egy éjszaka szórakozik különböző

vendéglátóipari egységekben melyeket kilenc, tíz, tizenegyes számmal láttam el. Péntek délután pedig egy fontos pont a Keleti Pályaudvar, ahonnan vonattal vidékre utazik. Hétvégéjét Egerben töltötte. Itteni lakhelye szintén könnyedén megállapítható GPS pozícióm alapján, illetve hogy szabadidejében különböző helyeket látogat meg, rövid egy-két órás intervallumban.

Összegezve lássuk mik is tudhatók meg róla kizárólag GPS koordináták alapján. Lakhelye, munkahelye, a munkával töltött idő hossza, iskolája, szabadidős tevékenységei, mint úszás, könyvtár, szórakozás. Emellett vidéki tartózkodási helye, közlekedési eszköz választása. Aránylag kis területet jár be – mint az a térképen is jól látszik – azt is gyalog vagy BKV segítségével. Amit pedig még fontosnak tartok, hogy mit nem csinál. Gondolok itt olyanra minthogy, vidékre nem a busszal való közlekedést választja, Budapesten nem részesíti előnyben a személygépkocsit, nem vásárol nagy hipermarketekben vagy, hogy nem kocsmázással tölti a szabadidejének nagy részét. Természetesen hosszabb távon való monitorozással, sokkal több információ tudható meg az adott felhasználóról. Valamint ezeket az adatokat kiegészítve hívás-, email-, SMS listával, böngészési előzményekkel vagy fényképekkel, életünk nyitott könyvvé válik.

Hölgy ismerősöm adatainak kiértékelését másfajta nézőpontból közelítettem meg. Hasonló információk nála is szinte teljes biztonsággal tudhatók, mint lakhelye, szabadidős tevékenységei vagy, hogy melyik felsőoktatási intézményben tanul, csupán az egy hetes feljegyzett adataiból. Azonban most azt taglalnám, hogy ezeket az információkat személyre szabottan mire és hogyan is lehetne felhasználni.

Nagy sikerek elsősorban a marketing területén érhetők el általuk. Gondolok itt a reklámozás minden féle-fajta módszerére, mint honlapokon vagy alkalmazásokban megjelenő hirdetésekre, melyek a felhasználó érdeklődési körének megfelelő termékeket, szolgáltatásokat promótálnak. Jelen esetben tudható, hogy a monitorozott személy sokat utazik mindennapjai során, így például könyvolvasással vagy zenehallgatással, nagy valószínűséggel szívesen tölti unalmas perceit. Lakhelyén és iskoláján kívül nem tartózkodik huzamosabb ideig heti rendszerességgel egyik helyen sem, ezáltal feltételezhetően, nem dolgozik. Továbbá mivel tudható, hogy a BGF Külkereskedelmi karán tanul, ilyen beállítottságú álláshirdetések is könnyedén felkelthetik a figyelmét.

Egy egyszerű felmérés alapadataiként is jól felhasználhatók a monitorozás által kapott információk, az adott személyek felkeresése és meginterjúvolása nélkül. Valamint ezáltal pontosabb tényadatokról beszélhetünk, nem zavarjuk fölöslegesen az adott személyeket, akik a sietségből eredő hibás-, vagy eltitkolni szánt információikkal torzíthatják a kutatás eredményét. Tegyük fel, hogy meg szeretnénk tudni, hogy a mai budapesti egyetemisták mivel töltik szabadidejüket. Egy jól meghatározott darabszámú mintavételből, és GPS pozíciók adataiból kimutatható, hogy mennyi időt töltenek sportolással, kocsmázással esetleg múzeumba vagy könyvtárba járással. Akár intézményekre lebontva tudható, hogy mennyit járnak be az adott iskolába, hol buliznak, vagy mivel közlekednek. Jelen esetben ez a következőképpen néz ki:

	Férfi	Hölgy	Átlag
Sportolás	3 óra	1,5 óra	2,25 óra
Bulizás	5 óra	6,5 óra	5,75 óra
Múzeum	-	-	0 óra
Könyvtár	1 óra	-	0,5 óra
Iskola	6 óra	21,5 óra	13,75 óra
Utazás (BKV, MÁV)	6 óra	9 óra	7,5 óra
Otthon	52,5 óra	59,5 óra	56 óra
Munkahely	20 óra	-	10 óra
ÖSSZESEN	93,5 óra	98 óra	95,75 óra

Természetesen nagyobb időintervallumon való adatgyűjtés nagyobb pontosságot eredményez, de már az így kapott információk is megdöbbentően sokat árulnak el az adott személyek szokásairól.

Kutatásom kiértékelésének a végéhez érve úgy érzem, hogy habár kis mintával és rövid intervallummal dolgoztam, már így is igazolódni látszanak Barabás Albert László szavai, az Interneten többek által felvetett elmélet, valamint a Raytheon cég munkásságának lehetőségei és veszélyei egyaránt. Jövőbeni tartózkodási helyünk rémisztően pontosan meghatározható. GPS adataink iszonyatosan nagy számú személyes információt közölnek, melyért túlnyomó részben az okostelefonjaink a

felelősek. Ezzel természetesen nem azt mondom, hogy meg kell tőlük szabadulni és más alternatíva után nézni, csupán jó tisztában lenni a tényekkel.

A sok negatívum után a következő fejezetekben megpróbálom kiegyenlíteni a mérleg másik oldalát. A témához kapcsolódó védelmi lehetőségeket, továbbá az okostelefonnal való adatgyűjtés előnyeit sorakoztatom fel, melyeket akár mi is tudatosan alkalmazhatunk mindennapjaink során.

9. VÉDELMI LEHETŐSÉGEK

Természetesen a felhasználónak lehetősége nyílik – különböző biztonsági óvintézkedések segítségével – egy megfelelő védelem kialakítására. Ezen fejezetben több módszer is bemutatásra kerül, amellyel megakadályozhatjuk készülékünkön tárolt adataink kiszivárgását.

9.1 Megelőzés

Android platformon a megelőzés módszerei lehetnek különböző telepíthető alkalmazások. Egyetlen hátulütőjük, hogy rendszergazda jogosultságok szükségesek hozzájuk – root-olni kell a telefont – amelyhez egy kis informatikai hozzáértés szükséges. Azonban ettől nem szabad megijedni, mivel az Interneten több olyan kézenfekvő leírás is található, mely egy hozzá nem értő számára is lépésről lépésre bemutatja a szükséges teendőket. Illetve tapasztalataim azt igazolják, hogy a közvetlen környezetében szinte mindenki talál a témában jártas ismerőst, aki szívesen segít, amennyiben elakadtunk. Visszatérve az alkalmazásokra, van köztük olyan, amelyik tűzfalként funkcionál, mint a Droidwall (Google Play) nevű applikáció. Ennek a segítségével a felhasználó készíthet egy listát, amelyben megadja, hogy mely programok nem létesíthetnek Internetkapcsolatot. Azonban ez csak a biztonság egy bizonyos fokát képezi, és az adatforgalom mennyiségének csökkentése a fő feladata. Kiegészítve egy blokkoló alkalmazással tökéletes párosítás. Ilyen például az LBE Privacy Guard (Google Play) nevezetű szoftver. Ezáltal programjainkat egyenként kontrollálhatjuk. Megadhatjuk, hogy egy alkalmazáson belül milyen funkciókat engedélyezünk vagy tiltunk le. Például a Facebook mobil változatánál letilthatjuk a check in funkciót, és ezáltal készülékünk nem küld GPS adatokat a szervernek.

Apple platformnál maga a cég garántálja a biztonság meglétét. Úgy vélik rendszerük hibátlan, a felhasználó megnyugodhat, eggyel kevesebb probléma, amivel foglalkoznia kell. Azonban a gyakorlat nem ezt igazolja, érdemes odafigyelni és ismert fejlesztők alkalmazásait telepíteni, ezáltal megelőzve adataink kiszivárgását.

9.2 Védelem nyílt WIFI hálózaton is

A négyes fejezetben – a hozzáértők számára aránylag egyszerű – WIFI hackelést szemléltettem. Ebben a részben leírom, hogyan tudnánk kivédeni egy esetleges Droidsheep támadást. Az első és legfontosabb, hogy ahol lehet a biztonságos https sémát használjuk, mint azt már korábban említettem is. Azonban különböző programokkal is növelhetjük esélyeinket. A Play áruházban fellelhető Droidsheep Guard alkalmazást erre a célra fejlesztették ki. Amint WIFI kapcsolatot észlel, automatikusan indul. A leírás szerint mindenféle ARP spoof támadás ellen használható. Amint nem megfelelő tevékenységet észlel, bontja a WIFI kapcsolatot, ezáltal óvva meg a felhasználót a támadástól. Természetesen ezt is kipróbáltam a gyakorlatban és tökéletesen működött. Amint elkezdtem a monitorozó tevékenységet, az a másik Androidos eszközön érzékelte azt és a hálózati kapcsolat bontásra került.

Apple iPhone-hoz való kifejezett ARP spoof elleni program nem lelhető fel az App Store-ban. Ez esetben alkalmazzuk a https oldalak használatát, valamint fontos tranzakcióinkat, illetve levelezésünket ne nyílt WIFI hálózaton bonyolítsuk.

9.3 Céges adatok biztonsága

A biztonság kérdése magánemberként sem megkérdőjelezhetetlen, azonban vállalati viszonylatban az egyik legfontosabb tényező. Egyre többen intézik munkahelyi levelezésüket okostelefonjuk segítségével. A Magyar Telekom Nyrt-n belül úgy vettem észre, hogy az emberek nagy százaléka Blackberry-t használ főként megbízható beépített biztonsági rendszere – BlackBerry Enterprise Server – miatt. Azonban egyre inkább elterjedté válnak az Android készülékek ezen a területen is. A Samsung, mint piacvezető okostelefon gyártó cég, felismerte az üzleti szférában rejlő lehetőségeket. A 2013-as barcelonai mobilkommunikációs konferencián mutatta be Samsung KNOX elnevezésű biztonsági megoldását. Teljes kompatibilitást és magas szintű biztonságot nyújt a cégeknek azáltal, hogy egyesíti a Nemzeti Biztonsági Szolgálat által

kifejlesztett, fokozott biztonságú Android platformot és az integritásmenedzsment szolgáltatásokat. A Samsung Mobil divíziója elnökének szavával élve „A Samsung KNOX egyensúlyt teremt a vállalati szabályozás és az alkalmazotti elégedettség között, azáltal hogy platform szinten alapvető biztonságot kínál, azonban nem csorbítja a felhasználói élményt.” (Wright 2013 saját fordítás) Ezen a téren a Samsung versenyelőnye valószínűleg nem tart sokáig. A többi mobilszolgáltató is előtérbe fogja helyezni ezt a fajta szemléletet és hamarosan előrukkol saját megoldásával.

10. AZ ADATGYŰJTÉS POZITÍV OLDALAI

Számtalan veszélyt, fenyegetettséget és negatívumot soroltam fel az okostelefonokkal illetve azok adatgyűjtésével kapcsolatban. Ebben a fejezetben bemutatom, milyen előnyökkel jár az, ha a cégek felhasználói adatokat gyűjtenek az ügyfelekről. Valamint, hogy ezt mi, tudatos felhasználók hogyan tudjuk alkalmazni, egy jobb mobil élmény érdekében.

10.1 Geolokáció

Tartózkodási helyünk adatai számtalan lehetőséget nyújtanak, mellyel megkönnyítik döntéseinket, mindennapjainkat.

10.1.1 Forgalmi információk

Tegyük fel, hogy sietős az utunk, Budapesten a dugó közepén állunk és azon morfondírozunk, hogy vajon melyik alternatív útvonalat válasszuk a gyorsabb haladás érdekében. Nem kell mást tennünk, mint bekapcsolni a korábban telepített magyar fejlesztésű közösségi navigációs alkalmazást, az Egérút applikációt és használni adottságait. Figyelembe veszi az ország forgalmi helyzetét, az utak járhatóságát, az útlezárásokat, valamint a forgalmat negatívan befolyásoló eseteket és ezen gócpontok elkerülésével navigál. Természetesen Internetkapcsolat megléte szükségeltetik a funkciók használatához.

10.1.2 Lopott autók felderítése

Egy másik hasznos szoftver a Traffic Club, mely egy közösségi információs rendszer. Segítségével a felhasználók megoszthatják egymással a tapasztalt sebességmérő kamerákat valamint forgalmi akadályokat, így az utazás során lehetőség nyílik elkerülni azokat. Nagy újítása a lopott autók felderítésének lehetősége. Nincs más teendőnk mit futtatni az alkalmazást, mely készülékünk kamerája segítségével monitorozza az előttünk haladó jármű rendszámát, mely egy algoritmus segítségével a rendőrség által feltöltött adatbázisból egyezéseket keres. Amennyiben lopott járművet érzékel, bejelentés történik az illetékes hatóság irányába, így megkerülhet az eltulajdonított gépjármű.

10.1.3 Egyéb

Emellett számtalan további lehetőség nyílik, például kerékpárosok közlekedési adatai alapján feltérképezhető, hogy hová érdemes bicikli utat építeni. Elhagyott készülékünk megtalálására, vagy rendőrségi felderítésekre lehet használni a különböző lokációs adatgyűjtéseket. Megmondható általuk, hogy merre járt az adott elkövető a kérdéses időpontban, illetve, hogy hol lesz megtalálható amennyiben – a már tudható – napi rutinját követi. Valamint a helyi aktuális időjárási adatok segítségével könnyedén megtervezhető napi viseletünk.

10.2 Fertőző betegségek terjedésének megjósolhatósága

Dirk Brockman az amerikai Robert R. McCormic mérnöki tudományegyetem társprofesszora egy merőben új szemszögből közelítette meg a vírusok és fertőző kórok terjedésének monitorozását. (Hubbard 2011) Modern technológia felhasználásával – mint geolokációs adataink elemzése – próbálja feltárni, illetve megjósolni ezen betegségek várható térhódítását. Az emberi mobilitást vette alapul, majd matematikai modellek segítségével építette fel teóriáját. Nincs másra szükség, mint az emberek utazási szokásait, illetve egymásra gyakorolt fizikai kapcsolatait vizsgálni, melyben a különböző okostelefonok, valamint közösségi szájtok nagy segítséget nyújtanak. Minél jobban megismerjük ezen összefüggéseket, annál hatékonyabban lehet fellépni egy esetleges járvány kezelése során.

10.3 Nemzetközi kutatás Szegeden

Egy 2013 év elején indult kétéves európai szintű kutatásról beszélünk. Hazánkban a FuturICT.hu nevű programot a Szegedi Tudományegyetem vezeti több projektcéggel segítségével. Céljuk az okostelefonok által generált hatalmas mennyiségű adattudományos célra való felhasználása. Kertész János akadémikus, a Budapesti Műszaki és Gazdaságtudományi Egyetem professzorának szavaival élve *“A társadalom, az emberi viselkedés soha nem látott tempóban változik. Ahhoz, hogy ezt a folyamatot nyomon tudjuk követni, és az emberi jólétet, annak kormányozhatóságát elő tudjuk segíteni, meg kell érteni a társadalmat és ezeket a változásokat – ez válik lehetővé az adatok tanulmányozásával”* (idézi: Arany 2013) Az adatok védelmére nagy hangsúlyt fektetnek. Anonim módon kezelik az információkat, valamint egy külön csoport foglalkozik az etikai kérdésekkel. Nagy kíváncsisággal tölt el a projekt jövőbeli alakulása, valamint a lehetőségek kihasználásának módja.

11. ÖSSZEFOGLALÁS

Dolgozatomban az okostelefonok adatgyűjtési módszereinek részletes bemutatására törekedtem, annak érdekében, hogy teljes képet kaphassunk ennek veszélyeiről, illetve pozitív oldalairól.

Az adatgyűjtésnek rengeteg fajtája és módszere létezik. A nagy mobilcégek, mint az Android, vagy az Apple; a mobilszolgáltatók, mint a Telekom, de fejlesztő cégek vagy magánszemélyek is szeretnének többet megtudni az adott ügyfélről. Leggyakoribb módszer a letöltött alkalmazás segítségével történő adatgyűjtés, de nyílt WIFI hálózaton keresztül is rengeteg információ szivároghat ki. Jobb esetben csak személyre szabott reklámok küldése érdekében használják ezeket, azonban magánszemélyeket könnyedén meglehet, hogy anyagi károkozás vezérli.

Itt kell különválasztani a legális és illegális adatgyűjtési változatokat. Legális feltételek megteremtéséhez szükséges a felhasználó beleegyezése, mely történhet a telefon aktiválásakor vagy alkalmazás letöltésekor, mely az Android platformra jellemző. Illetve az alkalmazás használata közben – a szükséges funkcióhoz tartozó oldalon – egy felugró ablakban mely az Apple sajátossága. Ezen engedélyek hiánya az

adatgyűjtést illegális tevékenységgé emeli, mely jogi következményeket von maga után.

Kategóriák szerint beszélhetünk névjegyadatok gyűjtéséről, ezáltal egy jól használható név, telefonszám és email cím lista áll rendelkezésre. Geolokációs adatgyűjtésről, amikor is a felhasználó aktuális tartózkodási helye, naplózás esetén akár heti rutinjai is könnyedén feltérképezhetők, valamint a jövőbeni pozíciója kellő pontossággal megjósolható. Böngészési előzmények, híváslisták és SMS-ek valamint felhasználónevek és jelszavak kiszivárgása esetén, szintén rengeteg személyes információ tudható meg az adott felhasználóról.

Dolgozatom által továbbá megtudhattuk, hogy a legnagyobb veszélyt a nyílt WIFI hálózatok jelentik, melyet egy gyakorlati példával is szemléltettem. Bemutatásra kerültek nagy érdekvédelmi szervezetek, illetve magánakciók, melyek a felhasználók érdekeit védik, valamint a cégeket és fejlesztőket kontrollálják. Az alkalmazások telepítéséhez szükséges engedélyek problémáit egy tíz fős minta összehasonlításával szemléltettem. Továbbá egy nagyobb volumenű kutatásból kiderült, hogy geolokációs adatok segítségével mennyi minden tudható meg az adott okostelefon tulajdonosáról.

Természetesen védelmi lehetőségeket is szemléltettem dolgozatomban. Mind magánszemélyek, mind céges módszereket sorakoztatok fel, egy biztonságosabb okostelefon használat érdekében

Végül, de nem utolsó sorban az adatgyűjtés pozitív oldalai kerültek bemutatásra. Rengeteg, a mindennapjaink során alkalmazható hasznos alkalmazás lát napvilágot. Melyek gyorsabb közlekedést, lopott autók felderítését vagy például elhagyott készülékek megtalálását teszik lehetővé.

Kutatók felismerték, hogy a felhasználókról tárolt, nagy mennyiségű adat, tudományos célra is fordítható, amit a Szegeden zajló projekt is jól igazol. Ez a terület még aránylag kiaknázatlan, ezáltal a jövő rengeteg lehetőséget kínál. Továbbá reméljük, hogy a biztonság még magasabb helyen fog szerepelni, és a védelmi lehetőségek tárháza folyamatosan gyarapodni, fejlődni fog.

Összegzésként, a jelenleg rendelkezésre álló információkból következtetve elmondhatjuk, hogy az okostelefonok világában történő adatgyűjtés kétélű fegyver. Egyik szemszögből vizsgálva a felhasználók legnagyobb ellensége lehet, mivel könnyedén visszaélés áldozatává válhatnak. Másik oldalról közelítve pedig egy

fantasztikus, sokféle felhasználási lehetőséget magában rejlő kiaknázatlan terület. Az még a jövő kérdése, hogy a mérleg mely oldala túlsúlyba kerülni. Szerencsére többen is felismerték a benne rejlő pozitívumokat és különféle lépéseket tesznek a fejlődés érdekében. Reméljük, hogy kezdeményezések, mint a szegedi kutatás jó irányba tereli az adatok kezelését valamint a felhasználás módját, és területét.

Irodalomjegyzék

Allan, Alasdair and Warden, Pete (2011) - *Iphone Tracker* -
<http://petewarden.github.com/iPhoneTracker/> (letöltve 2013. február 16.)

Arany Mihály (2013) - *Tüntetés- és forradalomszervezés a világhálón – avagy internethasználat ma* - <http://szegedma.hu/hir/szeged/2013/01/mirol-arulkodik-a-mobil-es-internethasznalatunk.html#more-271241> (letöltve 2013. március 16.)

Arthur, Charles (2011) - *Android phones record user-locations according to research* – The Guardian - <http://www.guardian.co.uk/technology/2011/apr/21/android-phones-record-user-locations> (letöltve 2013. február 16.)

Bilton, Nick (2012) - *Disruptions: So Many Apologies, So Much Data Mining* -
<http://bits.blogs.nytimes.com/2012/02/12/disruptions-so-many-apologies-so-much-data-mining/> (letöltve 2013. február 22.)

Bohn, Dieter (2012) – The Washington Post – *Carrier IQ taking steps to rebuild its reputation* - http://articles.washingtonpost.com/2012-05-08/business/35458518_1_carrier-iq-privacy-issues-privacy-policies (letöltve 2013. február 18.)

Cannon, Thomas (2011) - *No-permission Android App Gives Remote Shell* -
<https://viaforensics.com/security/nopermission-android-app-remote-shell.html> (letöltve 2013. február 23.)

Droidsheep – *How does this work?* - http://droidsheep.de/?page_id=424
(letöltve 2013. február 22.)

Eckhart, Trevor (2011a) – *CarrierIQ* -
<http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/> (letöltve 2013. február 18.)

Eckhart, Trevor (2011b) – *CarrierIQ Part 2* -
<http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/carrieriq-part2/> (letöltve 2013. február 18.)

Federal Trade Commission (2012a) - *Making Sure Companies Keep Their Privacy Promises to Consumers* -
<http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml> - (letöltve 2013. február 18.)

Federal Trade Commission (2012b) - *Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* - <http://ftc.gov/opa/2012/08/google.shtm> (letöltve 2013. február 18.)

Federal Trade Commission (2012c) – *Mobile Apps for Kids: Current Privacy Disclosures are disappointing pdf* - http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. (letöltve 2013. február 18.)

Gallagher, Ryan (2013) – *Software that tracks people on social media created by defence firm* - <http://www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence> (letöltve 2013. február 27.)

Gálffy Csaba (2012) - *Egymilliárd okostelefon-felhasználó van a világon* - <http://www.hsw.hu/hirek/49216/okostelefon-piac-microsoft-windows-google-android-apple-iphone-nokia-communicator.html> (letöltve 2013. február 13.)

Haselton, Todd (2011) – CNN – *Think Carrier IQ is bad? WikiLeaks founder says all smartphones can be hacked with ease* - <http://bgr.com/2011/12/02/think-carrier-iq-is-bad-wikileaks-founder-says-all-smartphones-can-be-hacked-with-ease/> (letöltve 2013. február 18.)

Houston, Thomas (2011) – *Google Is Tracking Android Users' Location Data, Say Researchers* - http://www.huffingtonpost.com/2011/04/22/google-android-and-apple-track-your-location_n_852529.html (letöltve 2013. február 16.)

Hubbard, Bethany (2011) - <http://globalhealthportal.northwestern.edu/blog/2011/08/a-qa-with-mccormicks-dirk-brockmann/> (letöltve 2013. március 6.)

Klenovszki János (2012) – NRC – *Fókuszban a mobilman* - <http://www.mobilhungary.com/prezentaciok/A-mobilpiac-szamai-es-a-mobilman-profilja/119/> (letöltve 2013. március 22.)

May, Patrick and Wolverton, Troy (2011) – *Your smartphone knows everything about you, and it tells tales.*: <http://phys.org/news/2011-05-smartphone-tales.html> (letöltve 2013. február 13.)

Microsoft – *A cookie-k ismertetése* - <http://support.microsoft.com/kb/260971/hu> (letöltve 2013. február 18.)

Mindentudás Egyeteme (2011) – *Az adat teszi az embert* - <http://mindentudas.hu/riportfilm/item/2804-az-adat-teszi-az-embert.html> (letöltve 2013. február 27.)

Mobile Word Congress (2012) - *Smart phone pictures cause privacy concerns* - <http://privacy.cytalk.com/2012/02/smart-phone-pictures-cause-privacy-concerns/> (letöltve 2013. február 23.)

Nolan, Dan (2013) – *Massive Google Play Privacy Issue* - <http://phetdreams.tumblr.com/post/42959902001/massive-google-play-privacy-issue> (letöltve 2013. február 20.)

Norton 2012 Cybercrime Report (2012) - http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf (letöltve 2013. február 10.)

O'Rourke, Hillary (2011) - *Malware, lost or stolen devices top mobile phone security threats* - <http://searchsecurity.techtarget.com/news/2240112175/Malware-lost-or-stolen-devices-top-mobile-phone-security-threats> (letöltve: 2013. február 15.)

Philips, Tom (2013) - *Parents refused refund by Apple after son spends £1700 on free iPad game* - <http://www.eurogamer.net/articles/2013-02-28-parents-refused-refund-by-apple-after-son-spends-1700-on-free-ipad-game> (letöltve 2013. március 23.)

Pintér Róbert (2011a) – *A telefonok elektronikus bűnösökkel álmodnak. Mobil használati trendek idehaza.* Konferencia előadás. Smartmobil 2011. 2011. április 6. <http://www.slideshare.net/probesz/pintr-rbert-mobil-trendek-smartmobil-2011> (letöltve 2013. február 16.)

Pintér Róbert (2011b) – *Az okostelefonok terjedése Magyarországon* – Információs Társadalom folyóirat 2011 1-4 szám, Gondolat Kiadó, Budapest http://www.infonia.hu/infotars/arch_2011.html (letöltve 2013. február 12.)

Shankland, Stephen (2011) - *Carrier IQ apologizes, drops threat to security researcher* - http://news.cnet.com/8301-30685_3-57331150-264/carrier-iq-apologizes-drops-threat-to-security-researcher/ (letöltve 2013. február 18.)

Sperry, Todd (2012) - *Smartphone apps can compromise kids' data, FTC says* - <http://edition.cnn.com/2012/12/10/tech/apps-children-data> (letöltve 2013. február 20.)

Szilágyi Árpád (2011) – *Az első okostelefon* - <http://netidok.postr.hu/az-elso-okostelefon> (letöltve 2013. február 16.)

Van Grove, Jennifer (2012) - *Your address book is mine: Many iPhone apps take your data* - <http://venturebeat.com/2012/02/14/iphone-address-book/> (letöltve 2013. február 22.)

VírusHíradó (2012) – *Rootkit repeta* - http://www.virushirado.hu/hirek_tart.php?id=1980 (letöltve 2013. február 18.)

Westernvelt, Robert (2011) – *Search Security - Top 5 mobile phone security threats in 2012* <http://searchsecurity.techtarget.com/news/2240112288/Top-5-mobile-phone-security-threats-in-2012> (letöltve: 2013. február 15.)

Wright, Rob (2013) - *Samsung Knox Brings BYOD Security To Android Devices* – <http://www.crn.com/news/mobility/240149443/samsung-knox-brings-byod-security-to-android-devices.htm> (letöltve 2013. február 28.)

A dolgozatban hivatkozott okostelefon alkalmazások

Droidsheep androidos alkalmazás - <http://forum.xda-developers.com/showthread.php?t=1593990> (letöltve 2013. február 22.)

Google Play áruház – *Adidas MiCoach*
<https://play.google.com/store/apps/details?id=com.adidas.micoach&hl=hu> (letöltve 2013. február 27.)

Google Play áruház – *CoPilot Live Premium Europe* (9.856 Ft)
<https://play.google.com/store/apps/details?id=com.alk.copilot.eumarket.premiueupan&hl=hu> (letöltve 2013. február 25.)

Google Play áruház – *DroidWall program*
<https://play.google.com/store/apps/details?id=com.googlecode.droidwall.free&hl=hu> (letöltve 2013. február 13.)

Google Play áruház – *Droidsheep Guard*
<https://play.google.com/store/apps/details?id=de.trier.infsec.koch.droidsheep.guard.free&hl=hu> (letöltve 2013. március 4.)

Google Play áruház – *Egérút*
<https://play.google.com/store/apps/details?id=com.alk.copilot.eumarket.premiueupan&hl=hu> (letöltve 2013. február 25.)

Google Play áruház – *Google Maps*
<https://play.google.com/store/apps/details?id=com.google.android.apps.maps> (letöltve 2013. február 25.)

Google Play áruház - *LBE Privacy Guard*
<https://play.google.com/store/apps/details?id=com.lbe.security.lite&hl=hu> (letöltve 2013. február 25.)

Google Play áruház – *NAVIGON Europe* (17.550 Ft)
<https://play.google.com/store/apps/details?id=com.google.android.apps.maps> (letöltve 2013. február 25.)

Google Play áruház – *Navitel Navigator*
<https://play.google.com/store/apps/details?id=com.navitel&hl=hu>
51bGwsMSwxLDEsImNvbS5uYXZpdGVsIl0. (letöltve 2013. február 25.)

Google Play áruház – *Nike+ Running*
<https://play.google.com/store/apps/details?id=com.nike.plusgps&hl=hu> (letöltve 2013. február 27.)

Google Play áruház – *Ndrive 10*
<https://play.google.com/store/apps/details?id=com.ndrive.android&hl=hu> (letöltve 2013. február 25.)

Google Play áruház – *Route 66 Maps* +

<https://play.google.com/store/apps/details?id=com.route66.maps5&hl=hu> (letöltve 2013. február 25.)

Google Play áruház – *Runkeeper*

<https://play.google.com/store/apps/details?id=com.fitnesskeeper.runkeeper.pro&hl=hu> (letöltve: 2013. február 27.)

Google Play áruház – *Sygic: GPS Navigation*

<https://play.google.com/store/apps/details?id=com.sygic.aura> (letöltve 2013. február 25.)

Google Play áruház – *TomTom Europe* (20.489 Ft)

<https://play.google.com/store/apps/details?id=com.tomtom.europe&hl=hu> (letöltve 2013. február 25.)

Google Play áruház – *Traffic Club*

<https://play.google.com/store/apps/details?id=com.nve.trafficclub> (letöltve 2013. március 6.)

Google Play áruház – *Waze social GPS traffic & gas*

<https://play.google.com/store/apps/details?id=com.waze&hl=hu> (letöltve 2013. február 2.)

Melléklet

1. számú melléklet: Alkalmazások összehasonlítása

	Route 66	Svgic	Waze	Egérút	Navitel	Ndrive	Google Maps	Navigon	Tomtom	CoPilot
Hardver vezérlők										
Hagybeállítások módosítása		x	x		x			x	x	
Fényképezés, videó készítés, hang rögzítése	x	x	x					x		
Tartózkodási hely										
Dűrva (Hálózat alapú)	x	x	x				x	x	x	x
Praciz GPS helymeghatározás	x	x	x	x	x	x	x	x	x	x
Helymeghatározó források létrehozása tesztelésre										x
Hálózati kommunikáció										
Teljes internet-hozzáférés	x	x	x	x	x	x	x	x	x	x
NFC kommunikáció engedélyezése							x			
Bluetooth kapcsolat létrehozása			x					x	x	
Személyes adatai										
Névjegyek olvasása	x	x	x		x		x	x	x	x
Névjegyek módosítása	x						x			
Naplófájlok olvasása	x	x						x		
Tárolás										
Sd-kártya tartalmának módosítása vagy törlése	x	x	x		x	x	x	x	x	x
Rendszerezők										
Rendszerbeállítások módosítása			x					x	x	x
Telefon alvásának megakadályozása	x	x	x		x	x	x	x	x	x
WiFi kapcsolt létesítése/bontása		x			x		x	x		
Időzóna beállítása					x					
Alkalmazás állandó futtatásának beállítása						x				
Bluetooth-felügyelet								x		
Futó alkalmazások lekérdése							x	x	x	
Bíltentvűzár letiltása							x		x	x
Felhasználói felület beállításainak módosítása									x	
Rendszerszintű jelzések megjelenítése									x	
A fiókjai										
Fiók hozzáadása vagy törlése							x			
Google fiók használata							x			
Google térkép (alkalmazások sign in engedélyezés)							x			
Díjköteles szolgáltatások										
Telefonszámok közvetlen hívása	x	x				x	x		x	
SMS üzenetek küldése					x	x		x		
Telefonhívások										
Telefon állapotának olvasása	x	x		x	x	x	x			x
Az Ön üzenetei										
SMS fogadása					x	x				
Fiókjai										
Ismert fiókok lekérdezése			x				x		x	
Google-szolgáltatások konfigurációjának beolvasása							x			
Konfigurált fiókok megtekintése							x			
Hardver vezérlők										
Rezgőegység vezérlése		x	x				x	x		x
Lámpa vezérlése								x		
Tartózkodási helye										
Hozzáférés a helymeghatározó szolgáltatások speciális parancsaihoz		x	x							
Hálózati kommunikáció										
Hálózat állapotának megtekintése	x	x	x	x	x	x	x	x	x	x
WiFi állapotának megtekintése	x	x			x	x	x	x	x	x
Adatok fogadása az internetről		x	x				x			
Rendszerezők										
Bekapcsoláskor automatikus indítás			x				x			
Nem törölhető üzenet szórása			x					x		
Háttérben futó alkalmazások bezárása								x		
Parancsikövek telepítése							x			
Alapértelmezett										
Biztonságos tároló elérésének tesztje	x	x			x	x	x	x	x	x
Híváslista olvasása	x	x			x		x	x	x	x
Híváslista módosítása	x						x			

2. számú melléklet: Kutatási anyagok

2.1 Férfi ismerős adatai

02. 18. Hétfő			
Cím	Időpont	Időtartam	Következtetés
Bp. Bocskai út 16.	8:00	0:30	Repülő mód OFF - Ébredés
Bp. Magyar Tudósok krt. 9.	8:30	8:00	Munkahely - gyalog - ebéd helyben
Bp. Kőrösy József utca 7-9.	16:30	0:30	Fehérvári úti vásárcsarnok - gyalog - Vásárlás
Bp. Bocskai út 16.	17:00	2:30	Lakás
Bp. Mátyóki út 9.	19:30	1:30	Uzoda - gyalog
Bp. Karinthy Frigyes út 26.	21:00	1:00	Pinyó klub - gyalog - Quiznight
Bp. Bocskai út 16.	22:00	2:00	Lakás - gyalog
Alvás	0:00	8:00	Repülő mód ON - Alvás

02. 19. Kedd			
Cím	Időpont	Időtartam	Következtetés
Bp. Bocskai út 16.	8:00	1:30	Repülő mód OFF - Ébredés
Bp. Fővám tér 8.	9:30	1:30	Corvinus - villamos
Bp. Bocskai út 16.	11:00	1:00	Lakás - villamos - Ebéd
Bp. Magyar Tudósok krt. 9.	12:00	4:30	Munkahely - gyalog
Bp. Bocskai út 16.	16:30	1:30	Lakás - gyalog
Bp. Futó utca 37-45.	18:00	5:00	Corvin bevásárlóközpont - villamos
Bp. Bocskai út 16.	23:00	1:00	Lakás - villamos
Alvás	0:00	8:00	Repülő mód ON - Alvás

02. 20. Szerda			
Cím	Időpont	Időtartam	Következtetés
Bp. Bocskai út 16.	8:00	1:30	Repülő mód OFF - Ébredés
Bp. Fővám tér 8.	9:30	5:00	Corvinus - villamos - ebéd helyben
Bp. Szabó Ervin tér 1.	14:30	1:00	Fővárosi Szabó Ervin Könyvtár
Bp. Kőrösy József utca 7-9.	15:30	0:30	Fehérvári úti vásárcsarnok - gyalog - Vásárlás
Bp. Bocskai út 16.	16:00	3:30	Lakás - gyalog
Bp. Mátyóki út 9.	19:30	1:30	Uzoda - gyalog
Bp. Bocskai út 16.	21:00	3:00	Lakás - gyalog
Alvás	0:00	8:00	Repülő mód ON - Alvás

02. 21. Csütörtök			
Cím	Időpont	Időtartam	Következtetés
Bp. Bocskai út 16.	8:00	0:30	Repülő mód OFF - Ébredés
Bp. Magyar Tudósok krt. 9.	8:30	8:00	Munkahely - gyalog - ebéd helyben
Bp. Kőrösy József utca 7-9.	16:30	0:30	Fehérvári úti vásárcsarnok - gyalog - Vásárlás
Bp. Bocskai út 16.	17:00	2:00	Lakás - gyalog
Bp. Belváros	19:00	4:00	Kocsmák - villamos
Bp. Bocskai út 16.	23:00	1:00	Lakás - villamos
Alvás	0:00	10:00	Repülő mód ON - Alvás

02. 22 Péntek			
Cím	Időpont	Időtartam	Következtetés
Bp. Bocskai út 16.	10:00	3:00	Repülő mód OFF - Ébredés
Bp. Keleti Pu.	13:00	2:00	vonattal vidékre
Eger Kallómalom út 40.	15:00	5:00	Lakhely - autóval
Eger, belváros	20:00	3:00	szórakozás - autóval (taxi)
Eger Kallómalom 68.	23:00	1:00	Lakás - autóval
Alvás	0:00	10:00	Repülő mód ON - Alvás

02. 23. Szombat			
Cím	Időpont	Időtartam	Következtetés
Eger, Kallómalom út 40.	10:00	2:00	Repülő mód OFF - Ébredés
Eger - Berva 1-es lakótelep	12:00	2:00	Nagymama - autóval - ebéd
Eger, Kallómalom út 40.	14:00	10:00	Lakhely autóval
Alvás	0:00	10:00	Repülő mód ON - Alvás

02. 24 Vasárnap			
Cím	Időpont	Időtartam	Következtetés
Eger, Kallómalom út 40.	10:00	2:00	Repülő mód OFF - Ébredés
Eger Kertalja u 20.	12:00	2:00	Nagymama - autóval - ebéd
Eger, Kallómalom út 40.	14:00	5:00	Lakhely - autóval
Eger, Vasútállomás	19:00	2:00	Vonattal pestre
Bp. Bocskai út 16.	21:00	3:00	Lakás – BKV
Alvás	0:00	8:00	Repülő mód ON - Alvás

2.2 Nő ismerős adatai

Hétfő			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	9:30	3:00	Repülő mód OFF - Ébredés
Bp. utazás	12:30	1:00	BKV
Bp. Dióssy Lajos 22-24.	13:30	5:30	BFG külker
Bp. utazás	19:00	1:00	BKV
Bp. Bokréta 11.	20:00	5:00	lakhely
Alvás	1:00	8:30	Repülő mód ON - Alvás

Kedd			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	9:30	3:00	Repülő mód OFF - Ébredés
Bp. utazás	12:30	1:00	BKV
Bp. Dióssy Lajos 22-24.	13:30	3:30	BFG külker
Bp. utazás	17:00	1:00	BKV
Bp. Futó utca 37-45.	18:00	5:00	Corvin bevásárlóközpont - villamos
Bp. Bokréta 11.	23:00	2:00	Lakhely – BKV
Alvás	1:00	8:30	Repülő mód ON - Alvás

Szerda			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	9:30	3:00	Repülő mód OFF - Ébredés
Bp. utazás	12:30	1:00	BKV
Bp. Dióssy Lajos 22-24.	13:30	7:00	BFG külker
Bp. utazás	20:30	1:00	BKV
Bp. Bokréta 11.	21:30	3:30	Lakhely - BKV
Alvás	1:00	8:30	Repülő mód ON - Alvás

Csütörtök			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	9:30	3:00	Repülő mód OFF - Ébredés
Bp. utazás	12:30	1:00	BKV
Bp. Dióssy Lajos 22-24.	13:30	5:30	BFG külker
Bp. utazás	19:00	0:30	BKV
Bp. Stáhly utca 13.	19:30	1:30	Kék lótusz – Jóga, masszázs szalon
Bp. utazás	21:00	0:30	BKV

Bp. belváros	21:30	1:30	Kocsmák - villamos
Bp. Bokréta 11.	23:00	2:00	Lakhely - BKV
Alvás	1:00	9:00	Repülő mód ON - Alvás

Péntek			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	10:00	10:00	Repülő mód OFF - Ébredés
Bp. Belváros	20:00	5:00	Szórakozás
Alvás	1:00	10:00	Repülő mód ON – Alvás

Szombat			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	11:00	2:00	Repülő mód OFF – Ébredés
Bp. Futó utca 37-45	13:00	3:00	Corvin bevásárlóközpont – gyalog
Bp. Bokréta 11.	16:00	8:00	Repülő mód ON – Alvás
Alvás	24:00	9:00	

Vasárnap			
Cím/koordináta	Időpont	Időtartam	Következtetés
Bp. Bokréta 11.	9:00	15:00	Repülő mód OFF - Ébredés
Alvás	24:00	9:30	Repülő mód ON - Alvás