HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Vizi Pál
vizip@rmki.kfki.hu

OKOSTELEFONOK BIZTONSÁGI KIHÍVÁSAI

Absztrakt

A haditechnika egyik legfontosabb és legérdekesebb kérdése a számítógépes hálózatok folyamatosan fejlődő eszközei biztonságos alkalmazásának megteremtése. A cikk kitér az új mobil okostelefonok gerjesztette kihívásra és megoldásra. A szerző áttekinti az eredményeket, a vizsgálati és kutatási módszerek helyét, szerepét, problematikáját a fentiek néhány kérdésében.

Designing a safe environment for a special operating place like continuously evolving computer networks and implementation is one of the very important and interesting questions of military engineering technology. Subject of this article is about some Smartphones generated challenges and solutions. The author gives an overview about methods, results of checking up, the system of research works and problems in point of view of some problems of above described questions.

Kulcsszavak: *okostelefon, mobil számítógépes hálózatok ~ smartphones mobile computer networks*

BEVEZETÉS

Szerző ebben a cikkében röviden összefoglalja a számítógépes hálózatok és azok támadásának újdonságait, különös tekintettel a globális méretű mobil Internettel ellátott okostelefonokra. Bemutatja az új eszközöket, azok lehetőségeit és arányát a számítógépes hálózatokban. Igyekszik összegyűjteni az új állapot alakította kihívásokat és ezek kutatási irányát. Megoldásokat keres és próbál nyújtani a felmerült veszélyekre.

SZÁMÍTÓGÉPES HÁLÓZATOK TÁMADÁSA

A számítógépes hálózatok támadása a számos különböző esetben szerepel szakirodalomban. A különféle diszciplínák alapvetően hasonlóan, de a saját specialitásuknak megfelelően értelmezik a témakört.

Az evolúcióban a támadás, a térnyerés a túlélés egyik feltételeként azonosított. Ha matematikai modellen leegyszerűsítjük támadóra és támadottra, akkor a klasszikus a róka-nyúl differenciálegyenlet-rendszer alapján a korlátlan támadó jelleg nem kifizetődő az egymástól globálisan függő, egymással szimbiózisban élő populációban. Tehát a világ, az emberiség jelen történelmi álláspontja szerint a támadást a jog alapvetően bűncselekménynek vagy katonai eszköznek tekinti. A támadás tárgya jelen esetben a számítógépes hálózatok.

A rendőrségi bűnmegelőzés szempontjából definiálva a számítástechnika szerepe a bűnözésben lehet:

- hagyományos bűncselekmények végrehajtása;
- digitális adattartalmak jogszerűtlen felhasználása;
- informatikai eszközök manipulálása;
- számítógépes hálózatok támadása.

A számítógépes hálózatok elleni támadás szereplői a jótól a rossz felé haladva az etikus hackerek, hackerek, crackerek. Céljuk a jogosulatlan belépés, adatok megszerzése (hacker) vagy ezen lehetőségek felderítése (etikus hacker), illetve rosszabb esetben adatok megváltoztatása, törlése és tönkretétele (cracker)

- információk megszerzése kémkedési céllal;
- vagyoni haszonszerzés jogosulatlan banki átutalással;
- vagyoni károkozás adatok törlésével;
- erkölcsi károkozás honlapok megváltoztatásával. [1]

A katonai szempontok szerint definiálva:

Számítógép-hálózati hadviselés helye az információs műveletekben a következőkkel írható le. A védelmi szektorban az információt két területen alkalmazzák. Egyrészt az információt, mint a vezetés eszközét használják fel a hadviselésben, másrészt az információt, mint un. nem kinetikus energiát felhasználó „fegyvert” alkalmazzák az információs műveletekben. Az információs műveletek alkotóelemei a következők:

- műveleti biztonság;
- katonai megtévesztés;
- pszichológiai műveletek;
- információs infrastruktúrák, vezetési objektumok fizikai pusztítása;
- elektronikai hadviselés;
- számítógép–hálózati hadviselés;

Kapcsolódó elemei pedig:

- polgári–katonai együttműködés;
- tömegtájékoztatás.

Az összetevő elemeken kívül az információs fölény kivívásában és fenntartásában fontos szerep hárul a vezetési információs rendszerekre és az összadatforrású felderítésre, melyek az információs műveletek támogató elemeit jelentik. [2]

A számítógépes hálózatok támadását, mint más hasonló információs műveletet komoly törvényi, jogi háttér szabályozza. Normál esetben jogszabályba ütköző tevékenységet végrehajtani, például lehallgatni csak szigorú törvényi feltételek mellett, az erre esetileg feljogosított állami szervek lehetnek jogosultak és az adatkezelés szintén szigorú előírásai vonatkoznak rájuk.

Napjaink új kihívása azonban az okostelefonok és a mobil számítógépes hálózatok kihasználása, exploitja.

OKOSTELEFONOK – SMARTPHONES, MINT A SZÁMÍTÓGÉPES HÁLÓZATOK TÁMADÁSÁNAK ÚJ ESZKÖZEI

Napjainkban a következő okostelefonok terjedtek el. Az egy gyártótól (Apple) származó IPhone, IPad és IPod termékek. Ezek arányaikban drágák. A több gyártótól származó hardveren egységesen működő Google Android nyílt rendszer alapú okostelefonok, relatíve olcsóak. Vagy a Microsoft zártabb rendszerű Windows Mobile verziói és a Symbian operációs rendszer, amely jellemzően napjainkra a Nokia készülékeken fut és valószínűleg a Microsoft fogja uralni ezt a terepet. Valamint a BlackBerry rendszerű mobilkészülékek, amelyek kellő biztonsággal rendelkezhetnek, de ennek ára van, amelyet a jó ár/teljesítmény igényű piac szűk része értékelhet, de mintha elrohanni látszana a többi megoldás a BB mellett.

Az jó ár/teljesítmény arány miatt tehát várhatóan a legdinamikusabban az Android rendszerek terjednek el. Bár a cikk írásának idején az Oracle pert indított a Google ellen az Android operációs rendszerben felhasznált, a Google állítása szerint részben nyílt rendszerként, részben licencszelt Sun Java alkalmazások kerültek beépítésre. [3] Az Oracle vásárolta fel a Sun-t és így a Java platform tulajdona is a kezébe került. [4] Bármi legyen is a per kimenetele, a legalább részben nyílt rendszerű operációs rendszer tűnik jelenleg nyerőnek. Annak ellenére, hogy a Microsoft a SkyPe felvásárlása után a Nokiával kötött szerződésével is legfeljebb a második lehet. [5] A nyílt rendszer jellemzője, hogy döntően több szoftver készül rá, és ezek jobban elérhetőek. A továbbiakban tehát az Androidon futó programok kerülnek górcső alá. Funkciójukban hasonló, vagy teljesen azonos szoftverek a többi operációs rendszereken is létezhetnek.

ANDROID PROGRAM ESZKÖZÖK

Hálózat szkenner

A Network Mapper program a szerzők szerint egy nagyon gyors szkenner hálózati adminisztrátorok részére, amely átvizsgálja a hálózatot az irodában és egy CSV fájlként exportálni tudja GMail-en keresztül, feltérképezi, hogy milyen eszközök vannak a LAN-on.

Tartalmaz egy portscannert biztonsági audit ellenőrzésére és egy MAC adatbázist a NIC gyártók azonosítására. Észlelni képes a tűzfallal ellátott és rejtőzködő számítógépeket. Nagyon hasznos, ha meg kell keresni egy windows/tűzfalat, ami nem látható a hálózaton. Előnyös, ha FTP, SSH, SMB stb. szervereket kell megtalálni a hálózaton, és segít diagnosztizálni a hibákat. A vizsgálat eredményeit, mint egy CSV fájlt lehet elmenteni,

amelyet Excel / OpenOffice / LibreOffice programokba lehet importálni. A leírása szerint „Azért készült, hogy gyors és megbízható legyen. Nem dob el semmit, és meg tud birkózni a 3G hálózatokkal is” [6]

Az erősáramú hálózatokban és a kismegszakítós biztosítóval rendelkező kis és nagyfeszültségű hálózatokban alkalmazott szakaszolás módszerével egy konkrét IP és MAC című gép megkereshető. Nem feltétlenül az Android Network Mapper fog ebben jeleskedni, de kisebb hálózati problémák megoldására alkalmas segédeszköz lehet.

Kamera programok

Valós idejű közvetítés - SECuRET Camera WiFi LiveStream

Video kamera stream közvetlenül egy okostelefonról, amely a Wi-Fi hálózaton valós időben nézhető és távolról irányítható egy web böngésző segítségével. Reklámja szerint használható baba felügyeletre, komolyabb felügyeleti eszközként vagy egyszerűen csak a móka kedvéért! Illetve, amit a leírás is tilt, illegális tevékenységre.

Adatfolyam valós idejű közvetítés egy Android telefon kamerájáról egy webböngészőre. Használata egyszerű mindenki számára, mert semmilyen konfigurációs beállítások nem szükségesek. A kamera vezérelhető, az állóképek vagy mozgó videók a böngésző segítségével készíthetők, érhetők el és letölthetőek. Java felületet igényel. Számos további beállítással testre szabható, a választható felbontás a 320x200 képponttól a kamera maximális felbontásáig terjed. A jelen változatot csak WiFi hálózathoz hirdetik, de a LogMeIn, a TeamViewer IP cím független protokolljainak ismeretében a saját vagy harmadik féltől származó fejlesztők a teljes Internetre kiterjeszthetik az elérési lehetőséget. További funkciók fejlesztés alatt, beleértve hang közvetítését.

Képes álcázott működésre érintőképernyő zár funkcióval, így a valódi működés nem észlelhető. Ez a már beépített funkció okozhat kellemetlenséget illetéktelen felhasználás esetén. A Livestream alkalmazás elérhető az Android Marketen is. [7]

Titkos exponálás - Super Spy Camera+

A fejlesztő célja egy olyan kamera program volt, amely nem árulja el a felvétel készítőjéről, hogy képet vagy videó felvételt készít. Az okostelefon normál képernyőjének mutatása közben ikonméretnyi vezérlőgombokkal és áttekintő képpel operál. Zárhangot sem ad ki. A képeket nem a szokásos DCIM alkönyvtárban tárolja, hanem egy véletlen elnevezésű és mélységű alkönyvtárban, amelyről azért tájékoztatja a felhasználóját. A „védelem” eme foka természetesen csak ez egyszerű kíváncsi szemek elől titkolja el a foto anyagot. [8]

A lopakodó működés miatt a fejlesztő a honlapján ki is zár minden jogtalan felhasználásból eredő felelősséget.

Vonalkód és eltérítés - Barcode

Barcode Scanner El tudja olvasni a hagyományos ár vonalkódokat, a kétdimenziós mátrixkódokat (UPC-A és UPC-E, EAN-8 és EAN-13, Code 39, Code 128, QR kód, Data Matrix, PDF 417, ITF) Segítségével megoszthatók a kapcsolatok, alkalmazások, könyvjelzők a QR-kód segítségével. A kapcsolatok megosztása engedély köteles. [9]

Veszélye, kihívása a vonalkód reklám eltérítés például nyomtatott fali reklámok eseten a plakát saját kódjának átmatricázásával. A támadó saját céljára irányit, ami lehet saját oldal. Vagy akár lejárató cél, azaz a támadó ellenfele oldalára ugrat. Azt akarja elérni, hogy pl. eljárás induljon az ellenfelével szemben. A matricák elhelyezése megvalósulhat leolvasást imitálva, vagy távolról, célba találó módszerrel, elkerülendő a lebukást a bekamerázott helyszíneken. Jelentősége a kis helyre viszonylag rövid ideig összpontosult sok potenciális leolvasó mobileszköz esetén van. Azaz például nagy létszámú ifjúsági események, sportrendezvények stb. alatt.

Távoli asztal programok

Az alább felsorolt programok a TeamViewer, LogMeIn, Remote Desktop Client for Android és a VNC client megbízható gyártóktól származó megbízható alkalmazásoknak tűnnek. A számítástechnikai történelem során számos olyan feltörést végeztek már, ahol kisebb módosításokkal betörésekre alkalmas módosítások születtek.

VNC client – hátránya, és egyben előnye, hogy közvetlen IP címekre képes eljutni, nincs mögötte egy szerverközpont, ahonnan routereken és tűzfalakon át lehetne eljutni a célgépig. A nyílt forráskódja miatt veszélyes lehet, mert rosszindulatú kezek káros irányban módosíthatnak bele.

Remote RDP (Remote Desktop Protocol) client – Teljes elérés, szöveg Copy / Paste a helyi és a távoli gép között. A lokális memóriakártya hozzáköthető a távoli számítógéphez, ahol a lokális zenefájlok a távolban lejátszhatók. A demo verzió nem jár le.

A fenti szoftverekre érvényes, hogy a tűzfalon port forwarding beállítása szükséges, viszont nincs a háttérben szerver.

DROID - VPN (Virtual Private Network) beépített Android VPN.

Xtralogic Remote Desktop Client - Távoli asztal ügyfél Androidra – billentyűzet, egér és képernyőelérés, teljes Microsoft Remote Assistance kompatibilitás. Tömörítéssel sávszélesség kímélő alkalmazás.

Wyse PocketCloud RDP/VNC – RDP, VNC vagy WMware protokollokkal képes kommunikálni

TeamViewer – létezik szerverközpont, így routereken és tűzfalakon át lehetne eljutni a célgépig, ahol nem is a célgépet érjük el közvetlenül, hanem a célgép van kifelé bejelentkezve ugyanarra a szerverre, amelyen keresztül a kapcsolat létrejön.

LogMeIn Ignition – Logmein saját accounton belül a regisztrált gépek névszerinti keresésére és belépésre biztosít lehetőséget. Teljes elérés a számítógép eszközeihez, nem csak a fájlelérések, hanem beleértve a hangcsatornákat is.

ShowMyPC Remote Support hozzáférés [10]

Veszély, hogy nem csak a nyílt forráskódúaknál várhatóak törések, amelyek szabad hozzáférést adhatnak gépekhez akár egy mobilnethez kötött izmosabb Android készüléken keresztül is.

OKOSTELEFON VESZÉLYEK

Védett WiFi – külvilág összekapcsolása

Az egyik veszély az okostelefon mobilnet szolgáltatós és belső védett wi-fi közti kapcsolódása. Ehhez többnyire célszerűen nyílt forráskódú távoli asztal programok módosításait használják, összekötve más teljesen legális programok illegális célú használatával. A felhasználható programokat a „Távoli asztal programok” fejezetben tartalmazza ez a cikk.

Az egyik legveszélyesebb lehetőség a védett hálózatok területén belül a tűzfalakon kívüli Internetre kapcsolás, routolás.

Online lehallgatás

Másik veszély az online lehallgatás, amelyet gyors reagálású döntéshozatalok eseten vethetnek be.

Alkalmas időzített megzavarásra is.

Idáig is be lehetett hallgatni mobiltelefonok közti beszélgetésekbe, különösen a 450MHz-es mobiloknál volt ez egyszerű. A hivatalos megoldás csak állami szervek számára adott, a telefon és a mobil hálózat erőforrásaival. Az internetes elérés növeli a lehetőségeket, mert a háttérben futhat egy alkalmazás vagy szolgáltatás, amely a GSM sávon folytatott beszélgetést

egyszerűen felveszi és továbbítja az Internetes elérésen, akár a beszélgetéssel egyidőben, vagy utána.

Okostelefon zombi hadsereg

Harmadik veszély egy ismert tűzfalon belüli rendszer fizikai területén belül került számos okostelefon, amelyek fel tudnak jelentkezni belső WiFi-kre vagy a külső mobil Internetre. Az elterjedtség arányai miatt zombi hadsereg leginkább Android tagokból állhat. Hosszabb idő alatt, előre megszervezetten komolyabb támadást lehetne végrehajtani néhány okostelefonnal, például egy több fős zárt ülés alatt. Megoldást jelenthet, ha az ülés alatt az okostelefonok akkumulátor nélküli állapotban a folyosón várakoznának, de a munkaszervezés miatt valószínűleg épp használatban vannak, prezentációra, naptári, előjegyzési funkciókra, jegyzetelésre, netán hangfelvételre, ha ezt engedik. Ha a hálózatról le is kapcsolják, és csak jegyzetelésre használják, az ülés végén újra rákapcsolódik a netre és a trójai programnak lehetősége van elküldeni az elmúlt időszakban rögzített anyag kivonatát.

Nagyobb veszély, ha a zárt ülés résztvevői már előre megírt anyagai okostelefon/tablet-en vannak és ezek célzottan előre leolvashatók például egy tőzsdei ármozgást befolyásoló helyen és időpontban. A támadók egy igazgatótanácsi ülés alatti stratégiai módosításokat az üléssel párhuzamosan hatástalaníthatnak, vagy fordíthatnak kedvezőtlen irányba. A notebookok, netbookok, tabletek és okostelefonok a felsorolás sorrendjében egyre valószínűbben kapcsolódnak és tűnhetnek fel zárt tárgyalások ideje alatt vagy annak időbeli közelében nyilvános mobil hálózatokon.

Adatforgalom korlát.

A kémkedés korlátja az adatforgalom és a sávszélesség korlát. A hirdetések adatmennyisége elviszi a forgalom 80%-t.

Megoldandó (volt) az kémkedéshez elegendő extra forgalom biztosítása a különböző, Internettel nem teljesen lefedett, nem együttműködő országok területén: FaceBook, Twitter (nem véletlen a régi "csipogó" névazonossággal).

Ezek a reklámokon keresztül a felhasználók saját zsebéből finanszírozott, önkéntes információ (es dezinformáció) közlő helyek. A jelen egyensúlyt a piac alakította ki. A szükséges reklámfolyam tartja fönn a kémkedők számára ingyenes és önkéntes adatáramlást.

Tehát a felhasználókra zúduló a felhasználó által kifizetett (!) adatfolyam tartja fönn a rendszert. Jól jár az ügyfél, mert megkapja az adatokat a normál ügy- és üzletmenetkor. Jól járnak a szolgáltatók, mert hozzájutnak a HW fedezetén túli nyereséghez és jól járnak a kémszervezetek is, mert az önkéntes-nyilvános adatokból jól tudnak szemezgetni. [11]

Pozíció meghatározottság

A legtöbb okostelefon rendelkezik pozíció meghatározó eszközökkel.

A cikk a komplex hálózatok matematikája fejezetben is foglalkozik a pozíció meghatározással és követéssel.

Pozíció GPRS,GPS, WiFI WLAN alapján meghatározható.

A GPS és a kiegészítő elemekkel ellátott AGPS pontos lefülelést, meglepést tesz lehetővé.

Célpontként: GPS pozícióra küldött megsemmisítés, futár, kommandó, rakéta, vagy IED (Improvised Exploding Device) stb.

Megtévesztő célpontként: a célpont szándékos megtévesztésre használhatja, ál-hamis (fake) célpontként, ha az általa feltételezett ellene irányuló akció során szándékosan fals pozíciót sugall, például az addig ismertként használt mobil eszközt egy logikusan kiválasztott vonatra, idegen autóra stb. helyezi, lehalkított módban. Ezzel ésszerűen nagyjából egyidőben egy másik mobilkészüléket kezd el használni, amelyet kis idővel előbb kapcsol be. Vagy egész egyszerűen egy vadonatúj készüléket vásárol.

Szinkronizációs problémák

Szinkronizációs problémák - asztali, laptop, notebook, netbook, tablet, palmtop vagy okostelefon szinkronizációk, e-mail szerver problémák.

A klasszikus matematikai alapprobléma egy elektronikus levél írásánál, ha a kiindulási gépen íródik a levél és ez nem kerül át a többi használatban lévő gépre, akkor az író lemaradhat egy adatfolyamról. Azaz ha egy másik gépen van épp, amikor az általa kezdeményezett levélre válaszolnak neki, de a válasz nem tartalmazza az általa írtakat, vagy rosszabbik esetben kárára MÓDOSÍTVA tartalmazza, akkor már komoly bajba kerülhet. Ezt a problémát áthidalhatja egy szerver, mint egy klasszikus webes e-mail, amely a kimenő levelet is elmenti. Míg a beérkezett leveleket a POP szerver tárolja, lehet(ne) hasonló, amely az elküldött levelet tárolja. Anélkül, hogy a küldőnek önmagának is kellene küldenie egy másolatot, hogy az általa küldött levelek megjelenjenek bármely általa használt gépen. Ezt kezdettől nem oldották meg az e-mail rendszerek. Mára túlhaladott, mert az egyéb kommunikációs lehetőségek felülmúlják, mint az azonnali üzenetküldők, vagy a közösségi oldalak.

Hiányosságok javítása

Becslést adhatunk a következőkre, hogy a zárt kódú rendszerek hiányosságait idővel közzéteszik, részben a dolgozók (80%), részben a véletlenszerű támadásokkal derítik fel (15%) vagy az abszolút váratlan esetekben derülnek ki (5%).

Kutatási eredményként talán megjegyezhető, hogy a nyílt forráskódú rendszerek forráskód állapotban áttekinthetőek, így szakemberek számára meggyőzően biztonságos programok keletkezhetnek. Ugyanakkor a nyílt forráskódú rendszerekbe a megfelelő helyeken rosszindulattal bele lehet módosítani és így máris egy trójai, vagy rés kerülhet be az eredetileg megbízható alkalmazásba, amely felfedezéséig védelem nélkül garázdálkodhat.

KOMPLEX HÁLÓZATOK MATEMATIKÁJA

Komplex hálózatok matematikája - Barabási Albert László erdélyi származású Amerikában élő magyar professzor. A vele készült riportban vetették fel neki, hogy kevesen tudják, hogy az internet és a mobiltelefon használatával milyen irtózatos mennyiségű adattömeget szolgáltatunk magunkról. A választ a könyvében találhatjuk meg: "Manapság jóformán mindannak, amit teszünk, marad digitális lenyomata valamilyen adatbázisban. E-mailjeinket megőrzik a szolgáltatók naplófájljai, telefonbeszélgetéseink pontos időponttal ellátott adatai ott nyugszanak a telefontársaságunk hatalmas merevlemezein" – írja Barabási Albert László - Villanások című 2010-es könyvében. [12]

Az emberek, akik a mobil okostelefonokat mobil internettel; a későbbiekben majd egyszerűen fogalmazva mobil kommunikációval ellátott eszközöket használják, mozognak a Földön. Mozgásuk közben a legkülönfélébb módon pozíciójukról információkat küldenek szerte, adatbázisokból kutathatóan. A jogszerű kutatásokkal is érdekes megfigyelések tehetők magukról az emberekről. A cikkben helyhiány miatt csak összefoglalva néhány eredmény.

Az emberek többsége az otthonuk és nappali tartózkodási helyük között mozog és e két helyen tartózkodnak a legtöbbet. Megfigyelték, hogy aki időben közelebb - ez úgy 20 és 30 perc – lakik, az a két fő tartózkodási helyen felül több időt tölt kisebb bolyongással e két hely közelében. Aki időben távolabb lakik, az sokkal kevesebbszer végez, „enged meg magának” egyéb bolyongásokat a munkanapokon. Ellenben éppen ők mozognak a szabadnapokon inkább távolabb. Itt a kertvárosi lét és a jómód korrelációjára lehet gondolni. Jellemzően a dolgozó átlagemberek a hétvégi illetve szabadságolási időszakban a szabadidős illetve üdülési övezeteket keresik fel. A rokonlátogatás is jól látható a mozgások statisztikájában, ahol

családonként jellemzően néhány más lakóövezeti helyet keresnek fel. Az üzletemberek mozgása jellegzetes. Általában egy-két, néha tízes nagyságrendbeli helyet keresnek fel. Repülőút esetén jellemzően repülőterek közelében „tűnnek el" a hálózatról és jelennek meg más repülőterek közelében, vagy jellemzően szállodai illetve irodai negyedekben, ha csak ott kapcsolják vissza a készülékeiket.

A számítógépes hálózatok támadása szempontjából ezek az információk döntőek és az egyes készülékek jellemzői, mint MAC address, oprendszer verziószám, használt e-mail címek, kommunikációs szoftverazonosítók alapján globális méretű számítógépes hálózati elemként funkcionálnak és támadhatóak.

Jelenleg tervezik a hackertámadások hagyományos fegyveres megtorlását, kilátásba helyezését.[13] Külön kutatási terület keletkezik így, amely az elrettentés vagy a (szándékosan) téves ellencsapás kérdésköre.

AZ ÚJ VESZÉLYEK KIHÍVÁSAI

A fentebb összefoglalt problematikák és programok sajátja, hogy a fejlesztők képesek és meg is közelítik olyan szoftverek fejlesztését, amelyek könnyen kiegészülhetnek valódi kémprogramokká. Például olyan komplexé, amely egyszerre közvetít és felvesz hangot és mozgóképet (akár takarékosan, csak akkor, ha épp aktuális), elküldi a GPS, vagy a mobiltornyok és WiFi-k kiegészítő információi alapján a pozíciót, monitorozni engedik a felhasználó billentyűzet leütéseit és a képernyőtartalmat, legyen az szöveg vagy kép illetve ezek kombinációja, sőt a pixelgrafikus képeken levő szövegeket OCR kiegészítőkkel karakteres formába is átdolgozzák.

A lehetőség mindenesetre ott van ezekben a készülékekben, együtt mozognak a hordozójukkal, tulajdonosukkal, aki akár lehet „célszemély", követve őt a normál üzemen kívül az üzleti, a munkahelyi titkok világába, továbbá a magánszférába a hálószobától a toalettig. Ha némi józanságra ébred a vásárlói társadalom, ragaszkodni fog a kameralencsék mechanikus eltakarásához, a mikrofon mechanikus némításához, az okostelefon valós árnyékolásához, például a fém cigaretta tartókhoz hasonló tokok, amelyek megvalósíthatják a kommunikációs csatorna frekvenciájára jellemző Faraday-kalitka árnyékolást. A technológiai kihívásokon túl pszichológiai és erkölcsi, de mindenesetre társadalomtudományi és bölcsészeti problémákat vetnek fel a jelenlegi technológia és a magánszféra új kihívásai. Mindezeken keresztül támadhatóak a számítógépes hálózatok és nem csak a technika, azaz a hardver és a szoftver, hanem az emberi tényező, ahol az ember a naiv, jószándékú, vagy alapvetően jószándékú felhasználó, aki ha néha ugyan csalafintán használna stikában fényképező programokat, amelyek a rendelkezésére is állhatnak, de a jóízlés megakadályozza ebben, önmaga éppen eshet áldozatául mások kémkedési szándékainak.

Ez az új kihívás a számítógépes hálózatok támadásának új dimenziója és bár a téma a nevéből fakadó definíció szerint szűkebbnek tűnik, ha katonai feladatra gondolunk, ahol az élőerő megkímélése a cél, akkor a nem halálos fegyverarzenálban fontos, új és egyre fejlettebb szerepe lesz-van a számítógépes hálózatok támadásában.

Kutatási eredményként megállapítható, hogy míg a hagyományos számítógép hálózati elemek alapvetően helyhez kötötten működtek, a jelen eszközei kiegészültek olyan mozgó készülékekkel, amelyeken keresztül nőtt az esély a helyhez kötött, jól védett eszközökbe bejutni.

Intelligens telefonok - buta alkalmazások

Különböző vállalkozások célozzák meg a belső felhasználóikat és ügyfeleiket okostelefon alkalmazásokkal, mint például az Apple iPhone és a Google Android. Sok ilyen alkalmazás anélkül készült, hogy alaposan figyelembe vennék az alkalmazásuk következtében kialakuló

biztonsági vonatkozásokat. Ezek megsértése mind az egyéni felhasználókra mind intézményekre, vállalkozásokra egyaránt hatással lehet. Támadóként kihasználhatják a kiterjesztett hozzáférést az érzékeny adatokhoz és hálózati szolgáltatásokhoz. Az előadás tárgyalja az újonnan megjelenő okostelefon alkalmazások üzemeléséhez kapcsolódó fenyegetéseket, és áttekintést nyújt a fenyegetések modellezésének folyamatairól.

Az előadás példaként végigvezet néhány alkalmazáson ahol a támadó szemszögéből bemutatja milyen típusú információkat képesek kinyerni, amelyek lehetővé teszik a további fejlettebb támadásokat. [14]

EMBERI TÉNYEZŐK

A számítógépes hálózatok támadása témában a fent leírtak alapján is levonható a következtetés, hogy az emberi tényezők döntő szereppel bírnak.

Az alábbiakban megkísérlünk összefoglalót, becslést és értékelést adni, továbbá néhány példát bemutatni a napjainkban élesben megvalósult okostelefonos számítógép hálózati eseményről.

Hackerek és crackerek, amatőrök és profik

Megpróbálhatunk egy becslést adni az alábbi tényezőkre, mint „hacker – cracker” vagy „önkéntes, profi és megfigyelő”. Ha a közelmúlt hírei a hacker és egyéb befolyásoló cselekményeket végrehajtók életkoráról igazak, akkor egy csúcsirányú 5-ös skálán a fiatalkorúak jellemzői az alábbi érdemjeggyel értékelhető:

Affinitásuk a következő irányokban, mint hacking: 4,5, cracking: 5, jogi ismeret 2 (a befolyásolt részéről) – 4 (befolyásoló részéről).

Tudásuk és képességeik: Tehetség 4.5, érzék 4, veszélyérzet és jogi tudás 2, amire csak a rendőrségi vagy személyes szabadság korlátozás kilátásba helyezése hat.

Várható, vagy már megvalósult a profi (katonai) szervezetek beépülése a fiatalkorúak közé. Ez még fiatal, önkéntes és finoman szólva rablóból lett pandúr tagokkal valósulhat meg, ahol az idősebb szereplők inkább a biztos hátteret, a gyors kivonást, visszavonulást támogatják. A beépített fiatalok 100% azonos habitust mutatnak, kell mutassanak, mint egy focicsapat, kivéve módosító akció idején.

Taktika: A hacker és cracker csoportok mutathatják magukat erősebbeknek, vagy gyengébbnek. Békeidőben gyengébbnek, felkészüléskor jóval gyengébbnek, vagy épp erősebbeknek mutathatják magukat, közte visszaesésekkel, de jól idomulva az elérendő célhoz.

A riválisi csoportok között spontán, vagy kívülről irányítottan kitörhet harc, ahol a külvilág járhat egyaránt jól vagy rosszul. Jól jár, ha "megeszik" egymást. Rosszul, ha a harcuk során megerősödnek, vagy egy újabb, erőteljesebb és erőszakosabb csoportosulás jön létre, amely elméletileg előre jelezhetően várható is.

Információk és dezinformációk közösségi médián, okostelefonok közreműködésével

A FaceBook-on illetve blogbejegyzésekben könnyen keletkeztethetők álhírek, dezinformációk. Maga a Facebook létrejötte is maga egy nagy álhír lenne, még egy játékfilm is készült róla. A lerágott csont „sufnicég”, két testvér, még ha igaz, akkor is mesébe illik. Szóba se jöhet az információs fölényre törekvés... Miért is maradt ily erősnek a Twitter és a FaceBook, valamint a jelenleg még háttérben felnövekvőben lévő Google közösségi csúcsalkalmazás?

Hillary Clinton szerint a hidegháború végén csökkentették a költségvetési támogatást, amely kommunikációs szempontból hatalmas károkat okozott. Ennek ellensúlyozására,

valamint a közelmúlt közel-keleti és észak-afrikai eseményeinek hatására az adminisztráció az internetes közösségi oldalakra helyezte a hangsúlyt és farszi, valamint arab nyelvű Twitter-oldalakat is indított. [15]

Éppen a mobil eszközök léte teszi lehetővé, hogy valós, friss hírértékű helyzetek kerüljenek fel közösségi médiára, azt elemezve, visszahatva információs harcosok befolyásolhatják a TÁVOLI csoportosulás működését. Mérsékelhetik vagy erősíthetik a hatásokat, információkkal vagy dezinformációkkal láthatják el a helyszínen levő mobil okostelefonokkal kommunikáló résztvevőket.

Az információs harcosok [16] várhatóan közel ötven virtuális identitást képesek kezelni egyszerre és igyekeznek befolyásolni valódi eseményeket a kibertéren keresztül.

Más cikkek pedig beszámolnak róla, hogy, „most már bizonyos, hogy a 2011 tavaszi szíriai forradalom egyik ismert alakjává váló, leszbikus Amina Arraf nem létezik, és egy Skóciában élő amerikai férfi írta a nő híressé vált blogbejegyzéseit. Ezt a férfi felesége e-mailben erősítette meg a Guardiannek. A hír hallatára többen is bírálták a férfit, aki azzal védekezik, hogy nem számított ekkora figyelemre."

Elhitték neki, hogy a helyszínen mobil internetes okostelefonnal van jelen. „Shakira szól az iPodomon" állította. [17]

Pszichológiai behatások

Az intrika mobbing, csúfolódás bullying, pszichomotorok ereje jelentős a közösségi hálózatokon és a mobil számítógépes hálózatok támadásával még áttekinthetetlenebbé válhat az emberek ilyen tulajdonságából fakadó tevékenység, vagy a szándékosan létrehozva utánzott ilyen eljárás.

Távoli diszciplínák

Napjaink jelenségei, akár szimpatikusak, akár nem, akár elfogadhatóak, akár megváltoztatandóak, de tények. A hétköznapi ember számara távoli diszciplínák összekapcsolására alkalmas példa a "valóvilág" kísérletek, ahol szimpatikus-erőszakos elfogadott viselkedésformák kutatása folyhat, részben közpénzből, részben a „köz" pénzéből, hisz önkéntes reklámfaló közönség előtt folyik.

Az eredmények felhasználhatók nagy populációk mozgatására, irányítására.

A "nyertes" részben "sajáterős", saját újonnan megszerzett tudása-tehetsége segítségével tör előre, részben előre szerződött forgatókönyvet követ.

Elszigetelt földrajzi, nyelvi, írásjeli populációk, világvallások esetében eltérő finomhangolt paraméterekkel végezhetnek műveleteket. Közelítő példaként az azonos franchise televíziós műsorok jól megfigyelhető terepek. A közösségi tartalom megosztó oldalakon, mint például a Youtube földrésznyi távolságokból tekinthetünk bele azonos nevű és célú műsorokba, és megfigyelhetjük a helyi sajátosságokat. Azon is elcsodálkozhatunk, ha kell ezen egyáltalán, hogy a videón látható emberek kezében ott vannak az okostelefonok, amelyek láthatóan Internet eléréssel is rendelkeznek, így mozgó részét képezik a globális számítógépes hálózatoknak.

ÖSSZEFOGLALÁS

Szerző cikkében röviden megpróbálta összefoglalni a számítógépes hálózatok és azok támadása egy szegmensének újdonságait, különös tekintettel a globális méretű mobil internettel ellátott okostelefonokra. Bemutatta az új eszközöket, azaz az okostelefonokat, ezek lehetőségeit és dinamikus arányát a számítógépes hálózatokban. Igyekezett összegyűjteni az új állapot alakította kihívásokat és ezek kutatási irányait. Megoldásokat próbált keresni és igyekszik nyújtani a felmerült veszélyekre.

Felhasznált irodalom

[1] Dr. Szabó Henrik - Számítógépes bűnözés - bunmegelozes.uw.hu/szamitogepes.pdf - (2011.06.20.)

[2] Dr. Haig Zsolt - Számítógép hálózati hadviselés rendszere az információs műveletekben http://www.hadmernok.hu/xx/06_Haig_Zsolt.pdf - (2011.06.20.)

[3] Dávid Imre: Rekordkártérítést kérhet az Oracle a Google-től

[4] http://computerworld.hu/rekordkarteritest-kerhet-az-oracle-a-google-tol-20110622.html - (2011.06.22.)

[5] Kodolányi Balázs: Az Oracle megveszi a Sun Microsystemst http://computerworld.hu/az-oracle-megallapodasra-jutott-a-sun-microsystems-szel.html - (2011.06.20.)

[6] Dávid Imre: A Microsoft ma jelenti be a Skype felvásárlását http://computerworld.hu/a-microsoft-ma-jelenti-be-a-skype-felvasarlasat-20110510.html - (2011.06.20.)

[7] Android Network Mapper http://www.androlib.com/android.application.org-prowl-networkmapper-xtDn.aspx - (2011.06.20.)

[8] Android Market › Photography › SECuRET SpyCam https://market.android.com/details?id=com.dooblou.SECuRETSpyCam - (2011.06.20.)

[9] Android Market › Photography › Super Spy Camera+ https://market.android.com/details?id=com.snoweye.spycamera - (2011.06.20.)

[10] Android Market › Shopping › Barcode Scanner https://market.android.com/details?id=com.google.zxing.client.android - (2011.06.20.)

[11] Sunalini Rana: 10 Best Android Remote Desktop Apps - SloDive - http://slodive.com/freebies/android-remote-desktop-apps/ - (2011.06.20.)

[12] Barabási Albert László - Villanások (Bursts) - Nyitott Könyvműhely, 2010 p4

[13] Háborús cselekedetnek minősülhetnek a komoly hackertámadások - http://htka.hu/2011/06/02/haborus-cselekedetnek-minosulhetnek-a-komoly-hackertamadasok/ - (2011.06.20.)

[14] Dan Cornell, Principle, Denim Group - Smart Phones with Dumb AppsNAISG HouSecCon - THE Houston Security Conference - http://houstonseccon.com/media/archives/hacking-track-presentations/ - (2011.06.20.)

[15] CNN Wire Staff - Voice of America internet site hacked by Iranians - http://articles.cnn.com/2011-02-22/world/iran.voa.hacking_1_voice-cyber-attack-muslim?_s=PM:WORLD - (2011.06.20.)

[16] Dr. Kovács László – Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben – Doktori értekezés - http://193.224.76.4/download/konyvtar/digitgy/phd/2004/kovacs_laszlo.pdf - p24 - (2011.06.20.)

[17] Visnovitz Péter: Lehet, hogy sosem létezett a szíriai forradalom leszbikus hőse - http://www.origo.hu/nagyvilag/20110608-amina-arraf-a-sziriai-forradalom-leszbikus-blogger-hose-portre.html - (2011.06.20.)