Zrínyi Miklós Nemzetvédelmi Egyetem
Bolyai János Katonai Műszaki Kar

SZAKDOLGOZAT

A KÉZI SZÁMÍTÓGÉPEK BIZTONSÁGA

Készítette:

Szávay István LBHBB371

Konzulensek:

Dr. Muha Lajos, Krasznay Csaba

2008

Köszönetnyilvánítás

A szakdolgozat elkészítéséhez nyújtott segítséget ezúton köszönöm konzulenseimnek Dr. Muha Lajosnak (ZMNE Informatikai kar), Krasznay Csabának (kancellár.hu), valamint Balogh Sándornak (KFKI Zrt.).

Tartalomjegyzék

Bevezetés

Az adatvédelem az egyik legfontosabb téma napjainkban. Olyan mennyiségű és minőségű adatok gyűlnek össze a munkánk során, amelyeknek elvesztése saját magunk számára bosszantó, de egy cég számára akár komoly üzleti kockázatot is jelenthet. A számítógépeken köztük a kézi számítógépeken tárolt adatok által hordozott információ *érték*, *melyről* minden esetben *gondoskodni kell*!

Napjainkban egyre több olyan eszközt fejlesztenek és használnak, amik a mindennapi életünket könnyítik, szolgálják. Ezek között megtalálhatunk különböző számítástechnikai eszközöket, a notebooktól kezdve a játékkonzolokon át a mobiltelefonokig. Ide tartoznak a kézi számítógépeknek nevezett személyes digitális asszisztensek[1] (továbbiakban: PDA). Ezek az eszközök már nem csak szórakoztatásra képesek, hanem egyre inkább elősegítik a korlátlan, kötetlen kapcsolatunkat, a munkával, embertársainkkal, és a világgal. Ez természetesnek mondható, de ezt a kapcsolatot beárnyékolja a fenyegetettség, aminek árnyát azok húzzák a fejünk fölé, akik adatainkat kívánják megszerezni, munkánkat szándékosan megnehezíteni, avagy pusztán csak „szórakozásból" akarnak kárt okozni.

Azok a cégek, vagy egyéni felhasználók, akik nem foglalkoznak az eszközeik biztonságával, olyan kockázatnak teszik ki magukat, amelynek elhárítására, megelőzésére időben, pénzben, presztízsben kevesebbet kellene fordítaniuk előzetesen, mint azután, hogyha már bekövetkezik a baj.

Az információ ugyan nem kézzel fogható, de létezik. A tárolt információ védelme, biztonságban tudása elemi érdekünk. Ennek ellenére egyes felmérések szerint a megkérdezett felhasználók többsége azt vallotta, hogy semmi olyasmit nem tárol a gépén, amit érdemes lenne komolyabban védeni!

Valóban így van ez?

Sajnos nem! Az adatainkkal kapcsolatban - mint az élet sok más területén - itt is igaz, hogy leginkább akkor fognak hiányozni, ha elveszítjük őket.

[1] **PDA**: Personal Digital Assistant = személyes digitális asszisztens. Egy olyan, tenyérben elférő számítógép, amely képes olyan alapvető feladatok ellátására, mint a notesz funkció, alap szintű Word, Excel kezelés, valamint audió és videó lejátszás.

A dolgozat célja, hogy megváltoztasson egy felfogást, hogy megismertessen egy hozzáállással. Az eszköz képességeinek vizsgálatával választ kapunk arra a kérdésre, hogy meg tudjuk - e óvni a bizalmas titkainkat ezeknek a készülékeknek a segítségével? Választ keresünk arra, hogy vajon a kézi számítógépünk használatakor biztonságosan építünk - e ki kommunikációs kapcsolatokat más készülékek, vagy hálózatok felé? Mi történik akkor, ha a támadás bekövetkezik? Meg tudjuk-e védeni a személyes adatainkat a készülékkel?

A következőkben elemzésre kerülnek a különböző veszélyhelyzetek, amelyek a kézi számítógépen tárolt adatokat fenyegetik. A megoldások, hogyan lehet őket megfelelő módon megvédeni a veszélyforrások és az esetleges támadási kategóriák figyelembe vételével.

A világban ma egyre növekszik az információ megszerzésére irányuló támadások mértéke és ereje. Azok, akik nem törődnek a védelemmel, sokkal előbb célpontokká válnak.

1. Fejezet

Miről szól ez a fejezet?

A bevezető fejezetben megismerkedünk a kézi számítógépekkel, a kifejlesztésük történetével és fejlődésük állomásaival.

1.1 A PDA

A PDA egy olyan tenyérben elférő, kisméretű számítógép, amelyet elsősorban személyes információk rögzítésére, feldolgozására, tárolására fejlesztettek ki és alkalmaznak. A kor gyors fejlődésének köszönhetően már egyre erősebb CPU[2] - val rendelkeznek, ami már lehetővé teszi a bonyolultabb feladatok elvégzését, például a grafikai számolásokat, vagy akár egy a lövedék ballisztikai jellemzőinek kiszámolását. A bővülő memóriakapacitásnak köszönhetően pedig egyre több adat eltárolására van lehetőség ezekben az eszközökben. Az eszköz méretétől fogva könnyen hordozható, rejthető, de ez a mozgásszabadság visszaüthet, mert ez által elvesztése, eltulajdonítása könnyebbé válik.

A PDA egy infravörös port vagy egy USB kábel segítségével csatlakoztatható más eszközökhöz, ami egyrészt segítség, másrészt biztonsági rést is jelent, hiszen nemcsak az adatok és a szoftver frissítése egyszerűsödik le, de az adatlopás, az adatok kiszivárgása is könnyebben valósulhat meg. A külvilág felé való kapcsolatok miatt ma már egyes gépekben Wi-Fi[3] és Bluetooth[4] rádió is van. Ma már az internetes hozzáférés is elérhető velük, valamint bármilyen egyéb program telepíthető rájuk.

Egyes típusaikban vonalkód olvasó is megtalálható, ami nagymértékben elősegíti a raktározásban, anyagbeszerzésben való felhasználásukat. Gyártják őket csepp és ütésálló kivitelben, valamint léteznek kifejezetten katonai felhasználásra szánt, az extrém és egyedi igényeket kiszolgáló típusaik is.

---

[2] A **CPU** (***C**entral **P**rocessing **U**nit – központi feldolgozóegység)* más néven **processzor**, a számítógép azon egysége, mely az utasítások értelmezését és végrehajtását vezérli, félvezetős kivitelezésű, összetett elektronikus áramkör.

[3] **Wi-Fi** : A **Wi**reless **Fi**delity angol kifejezés rövidítése, mely vezeték nélküli Ethernet hálózati kapcsolatot jelent. Több sebességű változata létezik, melyek 11 Mbps-től 54 Mbps sebességig terjednek.

[4] **Bluetooth**: A Bluetooth egy rövid távú vezeték nélküli kommunikációs szabvány, melyet rendszerint telekommunikációs eszközök használnak az egymás közti, valamint számítógépekkel, PDA - kal és más a szabványnak megfelelő kommunikációra képes eszközzel.

1.2 A kézi számítógépek története

A 80-as évek elején még nem léteztek kézi számítógépek, ezért általában mindenki határidőnaplóba vagy csak egy egyszerű füzetbe gyűjtögette a fontos telefonszámokat, címeket, a napi tennivalóit. Tizenöt évvel később az Apple cég piacra dobta digitális személyi titkárát, az első toll alapú PDA - t: a Newton[5]- t.

1. ábra

Egy, még ma is működő Newton grafikus kijelzője.

Az eszköz nem lett túl sikeres, méretei és súlya nem engedte meg elterjedését, ráadásul igen gyengére sikerült a beleépített kézírás-felismerési eljárás. Ami a legfontosabb, hogy akkor még a felhasználók nem tudták igazán, hogy mire használjanak egy ilyen eszközt.

A PDA – k második nemzedékére nem kellett sokáig várni. 1995 márciusában az amerikai Palm Computing elkészített egy szintén toll alapú PDA - t, a Palm Pilotot. Az Apple funkciógazdag Newtonjával ellentétben a Palm gyors és hatékony volt, viszont egyelőre csak egyszerűbb feladatokat láthatott el: jegyzetelésre, címjegyzék-karbantartásra, naptári bejegyezések és feladatlisták készítésére lehetett használni. Az eredeti Palm Pilot Professional 1megabájt RAM – mal rendelkezett. A Palm Pilot, ez a zsebben hordható kézi számítógép a maga csekély funkcionalitásával is igen gyorsan népszerűvé vált leginkább azért, mert a napi teendőket, jegyzeteket bármikor szinkronizálni lehetett az asztali számítógéppel. Azt is mondhatjuk, hogy a Palm Pilot a PDA - k második generációjának a szabványává vált, hiszen lehetőség volt a szinkronizálás az asztali géppel, valamint rendelkezett érintés érzékeny kijelzővel.

[5] Egy, még ma is működő Newton grafikus kijelzőjét pillanthatjuk meg élőben a következő linken: http://66.18.227.240:8080/screen/, 2008.10.03.

Javult a kézírás-felismerés és letisztult, egyszerű, célratörő szoftverekkel rendelkezett. Lehetőség volt számos külső eszköz csatlakoztatására, ezáltal használhatósága tovább növekedett. Egyszerű funkcionalitásával és kezelhetőségével kivívta a felhasználók elismerését. A folyamatosan fejlődő Palm OS operációs rendszer sohasem akart a PC-s világban hódító Windows-szerű felhasználói felület konkurenciája lenni, céljának továbbra is az egyszerű kezelhetőséget tartotta.

A Palm gépekkel párhuzamosan Európában is piacra került az angol Psion cég első menedzser kalkulátor kinézetű PDA - ja, a Psion Series 3a. A Psion gépekkel együtt fejlődött az akkor még EPOC névre hallgató Unix alapokkal rendelkező mobil operációs rendszer platform. A nagy piaci nyomással, valamint a színes és multimédiás gépek megjelenésével a Psion nem tudott versenyben maradni, viszont miután az EPOC rendszer elérte az ER5 verziószámot, akkor erre alapozva létrejött a Symbian platform.

A Microsoft is beszállt a versenybe a Windows CE nevű operációs rendszerével, és a későbbi Pocket PC a tenyérgépek harmadik nemzedékének lett az operációs rendszere.

Ezek a gépek a látványos színes megjelenítőjükkel, multimédiás képességeikkel és sok más szemet káprázta tó képességükkel tűntek ki. A verseny beindult, elkészült a Palm III sorozat, több memóriával, infravörös kapuval, még kompaktabb mérettel, színes megjelenítővel. Mindhárom cég (a Psion, a Palm és a Microsoft) tudta, hogy ez a hatalmas, még kiaknázatlan piac előbb-utóbb dübörögni kezd és minden ide szánt eszköznek operációs rendszerre lesz majd szüksége. A Palm, a Microsoft és a Symbian operációs rendszere együtt lefedi a mai PDA - piac 95 százalékát, ezért jelenleg Palm OS, Pocket PC és Symbian OS alapú gépeket különböztetünk meg. A Symbian OS meghatározó szerepet tölt be a mobiltelefonok piacán. Mára, köszönhetően az évtizedes fejlesztésnek több mint 200 millió telefon operációs rendszereként használják a világban. A Symbian a személyi számítógépekével összevethető funkciókra képes készülékek számára fejleszt és értékesít operációs rendszert.

Szó nélkül nem lehet elmenni az egyéb operációs rendszert alkalmazó eszközök mellett sem. A japán Sharp a 2000. évi CeBIT[6] alkalmával jelentette be elsőként, hogy egy Linux-alapú kézi számítógépet szeretne megjelentetni. A számítógép Lineo[7] Embedix disztribúciót futtató eszköz lett azért, mert teljesen nyílt, ingyenes és a fejlesztőknek nagyobb szabadságot engedélyez, mint a konkurens operációs

[6] A CeBIT a világ egyik legnagyobb informatikai szakkiállítása és vására.

[7] A Lineo a linuxos szerverekre specializálódott Caldera International leányvállalata.

rendszerek.[8] A PDA – k története az Apple Newtonjával kezdődött, és az akkor még gyenge lábakon álló készüléket két, PDA képességekkel rendelkező „ükunokája”, az iPod Touch és az iPhone készülékek követik napjainkban.

Az Apple cég 2001 októberében piacra dobott egy teljesen új médialejátszót: ez volt az iPod. Az első iPod hasonlóan nézett ki a ma kaphatóakhoz, de lényegesen kevesebbet tudott. Külsőleg szinte ugyanolyan volt, mint a mai elterjedt rokonai, de fekete-fehér kijelzővel készült. Ebből jelenleg négyféle verzió kapható a piacon: Shuffle, Nano, Classic és Touch. Az első iPhone-t 2007. június 29-én kezdték el árulni az Egyesült Államokban, az első 30 órában 270 ezer készüléket értékesített az Apple, és eddig valamivel több, mint hatmillió darab fogyott belőle. Érdekessége a készülékeknek, hogy egy teljes, flash memóriából futó OS X[9] rendszer fut rajtuk, 500 MB-os méretben. Ezt a méretet többek között a csak asztali gépeken használatos applikációk eltávolításával érték el.

1.3 Rövid technológiai fejlődéstörténet a kombó készülékekig

A PDA - k az elmúlt években rohamos fejlődésen mennek keresztül. Egyre jobban hasonlítanak, a laptopokra vagy inkább azt mondhatnánk, hogy egyre inkább közelítenek annak funkcionalitásához. Míg a laptopok egyre kisebbek lesznek, addig a PDA - k egyre többet tudnak, egyre nagyobb a teljesítményük és egyre szélesebb területen válnak alkalmazhatóvá.

A legtöbb modellben szerepel email és internet elérési szolgáltatás és az újabbak, a fejlettebbek már képesek UMTS[10] hálózathoz kapcsolódni esetleg rendelkeznek HSDPA[11] eléréssel is. Nem ritka ma már, hogy egy csúcs-kategóriás PDA akár 520 MHz sebességű Intel Xscale processzorral, 480 x 640 pixeles, 18 bites színmélység megjelenítésére képes kijelzővel, 128 MB beépített memóriával. Ezen felül

[8] Itt meg kell említeni, hogy a Symbian Alapítvány bejelentette, hogy elkészíti a Symbian OS - t nyílt forrásúvá, ezzel adva még nagyobb lökést az elterjedésének.

[9] Az Apple operációs rendszere.

[10] **U**niversal **M**obile **T**elecommunications **S**ystems, a GSM-rendszer utódjának szánt, annak infrastruktúrájára épülő mobil távközlési rendszer, amely alkalmas fénykép, zene, mozgókép, videoklip és internetes tartalom továbbítására. Irodalom jegyzék: [9] hivatkozás.

[11] **H**igh-**S**peed **D**ownlink **P**acket Access. Harmadik generációs mobilkommunikációs protokoll, melyet előszeretettel használnak világszerte mobil internet illetve egyéb nagy sávszélességet igénylő szolgáltatások kiszolgálására.

rendelkezhetnek WiFi elérési lehetőséggel is, a Bluetooth alapú rádiós átvitel pedig ma már alapfelszerelése ezeknek az eszközöknek.

Megtalálható benne a memóriabővítő foglalat, amibe memóriakártyákon kívül I/O perifériák is illeszthetők. Ezen tulajdonságok hihetetlenül sokoldalú felhasználhatóságát teszik lehetővé a PDA - nak. A fejlődésnek talán csak a méret fog határt szabni, hiszen még most is töretlen a fejlesztés a kézi számítógépek világában.[12]

Ennek a fejlesztésnek az egyik leglényegesebb állomása a kombó készülékek megjelenése. Ezek már egyaránt képesek kiszolgálni a felhasználók igényét a telefon funkciókra, ötvözni és egybegyúrni a kézi számítógépek minden adottságát, valamint teljesítményüknél fogva akár a legújabb 3 dimenziós GPS[13] szoftverek futtatását is végrehajtják.

1.4 Felhasználhatóság

A PDA - k napjainkban már számos funkcióval rendelkeznek és igen sokféleképpen felhasználhatóak. Dokumentumok olvasására, adattárolására, adatkezelésére, internet elérésre, e-mail lekérdezésére és küldésére, zenehallgatásra, videó nézésére valamint játékra és egyre inkább GPS navigációra. Emellett számos olyan alkalmazást fejlesztenek ezekre az eszközökre, amelyekkel hálózathoz tudunk kapcsolódni, azon keresztül vagyunk képesek bizonyos tartalmak, adatok eléréséhez és használatához.

Gyűjtő néven Personal Information Management (Személyes Információ Kezelő) alkalmazásoknak hívjuk a PDA - k legfontosabb alapszoftvereit. Platform függetlenül léteznek olyan felhasználói programok a készülékekhez, esetleg más-más néven, amik a következő szolgáltatásokat nyújtják: naptár, telefonkönyv, tennivalók és jegyzettömb.

A rengeteg telepíthető program között vannak szótár-, térkép-, projekt management-, irodai-, adatbázis kezelő-, multimédiás- és egyéb hasznos szoftverek.

[12] Irodalom jegyzék: [7] hivatkozás.

[13] **G**lobal **P**ositioning **S**ystem, a föld bármely pontjáról elérhető műholdas helymeghatározó rendszer.

2. ábra

Személyes Információ Kezelő szoftverek.

Ezeknek a nagy többsége már gyárilag telepítve van az eszköz ROM (Read Only Memory) tárolójába. Ennek a megoldásnak az előnye, hogy nem lehet "elrontani" vagy véletlenül letörölni őket, így a PDA teljes "emlékezetvesztése" után is rendelkezésre állnak. További előny, hogy a kézi számítógépekre jelenleg még kevés internetes veszedelem (vírusok, trójaiak, férgek, stb.) leselkednek, de ezek a veszélyeztetések egyre fokozódnak.

Ahhoz, hogy a zavartalan működést biztosítsák, a hardvernek folyamatos energiaellátásra van szüksége. Ezt egy beépített fix, vagy cserélhető akkumulátor biztosítja, amiknek a segítségével, egy feltöltést követően 3-7 napig üzembiztosan képesek működni ezek az eszközök.

Az adatbevitel problémáját megszüntetendő, a készülékre számos, akár testre szabható kézírás-felismerő szoftver készítettek, vagy akár külső billentyűzetek csatlakoztatására is lehetősége van a felhasználóknak.

1.5 Pillantás a jövőbe, a típus jövőbeni térnyerése

A közeljövőben olyan fejlesztéseken mehetnek át ezek a készülékek, amik nagyban befolyásolhatják a típus jövőjét. A módosítások középpontjában még inkább előtérbe kerül majd a jó kezelhetőség, azon belül is az érintőképernyő minél teljesebb kihasználása.

A hagyományos (single-touch) érintőképernyők mellett már egyre több fejlesztés irányul a multi-touch rendszerű (azaz több érintési pont szimultán érzékelésre alkalmas) érintőképernyőkhöz, ami számos ötletes, de mindenképpen látványos grafikus funkcióval gazdagítja majd a kézi számítógépek kezelői felületét.

Az Apple nemrég levédetett egy új technológiát, amivel a hordozható készülékekbe szerelhetnek napelemeket. Az újítás nagyon valószínű, hogy az érintőképernyős kütyükbe, vagyis a Touchba és az iPhone-ba fog kerülni.[14]

A kézi számítógépek tudása folyamatosan növekszik, és szolgáltatáskészletük pedig egyre bővül. Habár a programozói eszközök következő változata lehetővé teszi majd a mérnökök számára, hogy könnyen létrehozzák az asztali alkalmazások mobil változatait, figyelembe kell venni a PDA - k eladásának csökkenését, miután a hasonló funkciókat kínáló mobiltelefonok elviszik a piacuk egy részét.

Manapság egyre inkább a telefonokban jelenik meg a legtöbb innovatív fejlesztés, így ezek a készülékek lesznek a digitális konvergencia zászlóshajói.

A mobiltelefonok csakúgy, mint a PDA – k, már WiFi kapcsolattal internetezésre is alkalmasak. Kézenfekvő tehát, hogy a mobil eszközök egyesítik magukban a digitális fényképezőgépek, videokamerák, zenelejátszók és számítógépek adottságait, ahogyan egyre fejlettebb képességekkel bírnak.

Az okos telefonok és a PDA - k tulajdonságai már annyira azonosak lettek, hogy nem érdemes külön venni a két kategóriát, összefoglalóan kézi-számítógépeknek hívjuk őket.

[14] Irodalom jegyzék: [10] hivatkozás.

2. Fejezet

Miről szól ez a fejezet?

Ebben a fejezetben megismerkedünk a biztonsági kockázat meghatározásával, valamint bemutatásra kerülnek azok a fenyegetés típusok és sebezhetőségek, melyek leginkább jellemzőek a kézi számítógépek világában.

2.1 A biztonsági kockázat értelmezése

„A biztonság kockázatalapú megközelítése abból indul ki, hogy a biztonság egy dinamikusan változó, kedvező - a követelményeknek megfelelő - állapot, amelynek megváltozása nem valószínű, de nem is lehet kizárni. Vagyis minél kisebb a változás valószínűsége, annál nagyobb a biztonság. A tökéletes biztonság a gyakorlatban szinte sohasem érhető el, mindig számolni kell valamilyen kockázattal és a védelmi intézkedéseket a kockázatok elemzésére kell építeni.”[15]

Éppen ezért a tökéletes biztonságra való törekvéssel lehet elérni azt az állapotot, amit a „biztonságos” kifejezéssel tudunk leírni, hiszen a gyakorlatban szinte sohasem érhető el a tökéletes biztonság, mert mindig számolni kell bizonyos fokú kockázattal.

Egy olyan környezetben kell helyt állniuk ezeknek a készüléknek, ahol még az informatikai vezetők többsége is fittyet hány a mobil eszközök biztonságára.

A PDA használata vállalati környezetben sokkal kockázatosabb, mint például a notebookoké, és habár a felhasználók túlnyomó többsége kockázatosabbnak tartja a PDA – kat a notebookoknál, mégis csak elenyésző részük tesz valamit az eszközön található adatok biztonságos használatáért, a többségük pedig nem titkosítja, nem védi az állományait.

Mindemellett a legtöbb felhasználó úgy tud a mobil eszközéről a vállalati hálózathoz csatlakozni, hogy a folyamat során azonosítás nem történik, így ha a PDA idegen kézbe kerül, a tolvaj nem csak a készüléken tárolt bizalmas adatokhoz juthat hozzá könnyedén, hanem lehetőséget kap a vállalati hálózat hozzáféréséhez.

[15] Munk Sándor: Információbiztonság vs. Informatikai biztonság. Robothadviselés 7. Tudományos Szakmai Konferencia 2007. november 27.

Hiába léteznek biztonsági előírások az informatikai eszközök használatára vonatkozóan, ha az vagy nem terjed ki a mobil eszközökre, vagy betartásuk, betartatásuk nem megfelelően történik meg.

A biztonság megvalósításának lépései a fenyegetések kiküszöbölésére kell, hogy irányuljanak, mégis sok esetben nem is lehetséges a kockázatok teljes, vagy nagymértékű kiküszöbölése. Ehhez tisztában kell lenni a sebezhetőségekkel, a fenyegetésekkel, valamint azzal, hogy ezeket milyen védelmi intézkedésekkel lehet mérsékelni, megakadályozni.

Léteznek azonban olyan fenyegetések, amiket nem tudunk előzetesen kezelni. Ezért tudnunk kell, mi a biztonság alanya. Ez pedig az információ, amelyet a PDA – n tárolt adatokból nyerünk.

Fontos, hogy ezt az információt illetéktelenek ne ismerhessék meg, kizárólag csak az arra jogosultak érjék el, és hogy az információ ne vesszen el, vagy semmisüljön meg, illetve semmiképpen ne módosuljon.

A Közigazgatási Informatikai Bizottság 25. sz. ajánlása (3.2 pontja) rögzíti, hogy a támadás és a védelem az információkat hordozó adatra irányul.

„… A kockázatelemzésen alapuló módszer egy olyan modellen nyugszik, amelynek a középpontjában a védendő alapérték, az informatikai rendszerben kezelt adatok által hordozott információk állnak. Ezeket a környezetüket alkotó rendszerelemek veszik körül. A támadások általában nem közvetlenül érik az adatokat, hanem az azokat "körülvevő" rendszerelemeken keresztül.

A fenyegető tényezők, illetve veszélyek az informatikai rendszerelemekhez kapcsolódnak és azokon keresztül okozhatnak károkat mind a kezelt adatra, mind az alkalmazásra, miután az informatika-alkalmazás függ a rendszerelemektől. Éppen ezért valamennyi olyan rendszerelemet vizsgálni kell, amelyektől az informatikai rendszer működése és valamilyen módon az alkalmazásai függnek, és amelyeket valamely fenyegető tényező vagy veszélyforrás közvetett, illetve közvetlen módon érinthet."[16]

A számítástechnika fejlődésével egyrészt az információ védelme korszerűsödik, másrészről a védendő információ jellege is óriási változásokon megy keresztül. A számítógépes hálózatok fejlődése tovább forradalmasítja az információ gyűjtését,

[16] A KIB 25. számú ajánlása: 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV) 1.0 verzió. (214. oldal)

feldolgozását, kezelését és tárolását, de ezzel együtt a támadások száma és minősége a számítógépes környezetben tárolt adatok megszerzésére is egyre fokozódik, fejlődik.

A biztonság és védelem értelmezése fokozatosan kiterjedt az információkat kezelő és az információs tevékenységeket támogató rendszerekre is, ezért a kézi számítógépek biztonsági kérdését leginkább három fő veszélyforrás köré csoportosíthatjuk:

Az első a készülékhez való idegen, jogosulatlan ***fizikai*** **hozzáférés**. Mivel ezek az eszközök elég kisméretűek, ezért könnyebb őket elveszíteni illetve ellopni. Egye becslések szerint több százezerre tehető azon készülékek száma évente, amelyet elveszítenek, vagy ellopnak. Ez azért problémás, mert a dolgozók harmada az üzleti, céges adatokat, esetleg a jelszavait, PIN[17] kódjait tárolja a készüléken. Ebből adódik a tárolt adatokhoz való ***jogosulatlan*** **hozzáférés,** amikor egy olyan személy képes hozzáférni a tárolt adatokhoz, akinek nincs arra jogköre, hogy ezt megtehesse. Minél több adatot tárolunk egy helyen, annál valószínűbb az „érzékeny" adat jelenléte. Mivel az adatok tárolási mérete folyamatosan növekszik, ezért a kézi számítógépek tárolókapacitása is követi ezt a memóriakártyákon keresztül. Azok az adatok, amik a hordozható eszközre rákerülnek, sokszor a vállalat tulajdonát képezik, és sok esetben nem is tud arról az IT felelős, hogy ezek az adatok kikerültek a felelősségi köréből. A kézi számítógépek már csaknem minden típusa rendelkezik valamilyen vezetékmentes hálózati kapcsolathoz való csatlakozás lehetőségével. Amennyiben a vezeték nélküli kapcsolat nincs megfelelően konfigurálva és használva, akkor az ***idegen*** **hozzáférés**, az adatfolyam lehallgatása biztonsági kockázatot jelent.

Tisztában vagyunk azzal, hogy a PDA – k és okos telefonok is számítógépek (még ha kisméretűek is), ezért programhibák, rosszindulatú szoftverek, vírusok, férgek, trójaik, hátsó kapuk okozhatnak rajtuk adatvesztést, vagy fokozhatják a sebezhetőségüket. Ezek érkezhetnek e-mailben is, de a Cabir[18] féreg óta tudjuk, hogy már Bluetoothon keresztül is terjednek. A „`SUPER_HALYAVNYE_SMS_MMS.jar`" nevű trójai pedig a felhasználó engedélye nélkül képes sms üzenetek szétküldésére a megfertőződött PDA készülékről.[19]

---

[17] **PIN**: (**P**ersonal **I**dentification **N**umber = személyi azonosító szám) egy 4 számjegyből álló titkos kód, amellyel különféle személyes jellegű szolgáltatásokat védenek. Legközismertebb alkalmazásai a folyószámla-hozzáférés (bankkártyák) és mobiltelefon-használat korlátozása.

[18] A Symbian operációs rendszert futtató telefonokat fertőzi meg, és egy SIS formátumú, biztonsági felügyeleti szoftvernek álcázott fájl segítségével terjed.

[19] Irodalom jegyzék: [13] hivatkozás.

2.2 Tipikus fenyegetések

2.2.1 Social Engineering

Egy közhelyet idéznék, amely szerint „Minden lánc olyan erős, mint a leggyengébb láncszeme”. Ez helytálló a kézi számítógépek biztonságának világában is. Hiába használjuk a legújabb csúcstechnikát, elég egy hajszálvékony rés a védelemben, és máris elveszíthetjük az uralmat a rendszerünk felett. Az igazat megvallva, még manapság is a biztonsági lánc leggyengébb láncszemét alkotó elem nem szilícium,[20] hanem szén alapú létforma, maga az ember.

Röviden megválaszolva, a Social Engineering az emberek természetes, bizalomra való hajlamának kihasználása. Ez a támadási fajta nem a hardverelemek, a szoftver vagy a hálózat hibáit, hanem az emberi természet gyengeségeit használja ki az információ megszerzésére. Egyáltalán nem elfogadható az a megközelítés, hogy bizalommal kell lenni az emberek iránt, hiszen - és itt megint egy közhely következik - a pokolba vezető út jó szándékkal van kikövezve. Az emberi viselkedést megvizsgálva megállapíthatjuk, hogy ha elég kitartóan próbálkozunk, találunk valakit, akinek a hiszékenysége a mi malmunkra hajtja a vizet. A támadók ki is használják ezt az alapvető emberi tulajdonságot. Egy valamennyire hihető történet, vagy kellően magabiztos fellépés esetén valószínűleg lesz valaki, aki a szükséges információt a támadó rendelkezésére bocsájtja. Az emberi természetnek ezt a kihasználhatóságát társasági manipulációnak, angolul Social Engineering - nek nevezik. Ez nagy szerepet játszik abban, hogy a támadó megkerülhesse a biztonsági korlátokat, amiket a tűzfalak és egyéb behatolás-érzékelő rendszerek bonyolult, gyakran csak nagy erőfeszítések árán kijátszható rendszerei alkotnak. A felhasználók hiszékenységére vagy az éberségük hiányára alapozva gyakran könnyű behatolást tesz lehetővé ez a támadási forma.

Általánosságban elmondható, hogy a Social Engineering támadások ugyan eltérőek egymástól, de mindnek megvan a forgatókönyve, egy olyan mintája, amelyet minden, ilyen jellegű támadás használ.

Ezek:

- Információszerzés
- Kapcsolatépítés

[20] Az informatikai iparban a számítógépek processzorait (CPU) szilícium lapkák alkotják.

- A kapcsolat kihasználása (felhasználása)
- Végrehajtás – a tervezett cél megvalósítása.[21]

Az *információszerzés* célja, hogy a *kapcsolatépítéshez* megszerezze a lehető legtöbb és legjobb információt, ezáltal a kiépítendő kapcsolat minél használhatóbb legyen a támadáshoz. Ez igen sok időráfordítást, valamint előzetesen jól kidolgozott ötletet és tervezést kíván meg a támadótól. Ennek során használhat telefonos megkeresést, célzott elektronikus levelet vagy kukaátvizsgálást értékes információk után kutatva.

A kapcsolatépítés folyamatában a kiválasztott személyt, olyan pszichológiai támaszokkal látják el, amitől motivációt kap, hogy akarata ellenére segítségre legyen. Ezek olyan megerősítést nyújtanak számára, mellyel azt képzeli, hogy a felelőssége elhárítható, esetleg vágyat kelt benne, hogy cserébe kaphat valamit, vagy a morális bűnösség elkerülésének érzetével kecsegtet.

Mindemellett kézenfekvő, hogy az embert a tudatlansága is belesodorhatja, kíváncsisága is hajtja, esetleg gondatlanságból, vagy bosszúvágyból követi el azt a hibát, amire a támadónak célja eléréséhez szüksége van. A támadónak fontos, hogy a célszemély bizalma, pontosabban ő maga kihasználhatóvá váljon a későbbiekben.

Jobban belegondolva egy ilyen jellegű támadás naponta megeshet anélkül, hogy észrevennénk. A munkatársunk kölcsönkéri a PDA - nkat, mondván, hogy csak egy e-mail üzenetet szeretne elküldeni róla, mert otthon felejtette a sajátját. Magunkkal visszük szórakozóhelyekre (ez főleg kombó készülékeknél igényel fokozottabb elővigyázatot), ahol megkérjük rá a barátainkat, hogy vigyázzanak rá, amíg táncolunk.

Bármilyen olyan esetben, amikor a készülék kikerül a tulajdonosának, jogos használójának irányítása alól, akkor érheti Social Engineering támadás. Ez a fajta biztonsági sebezhetőség megelőzhető akkor, ha éberebben, nagyobb odafigyeléssel védekezünk a legnagyobb veszély, az emberi természet ellen.

[21] A rendszer próbája: az etikus hackelés és penetrációs tesztelés, Krasznay Csaba, 2007

2.2.2 A vezeték nélküli adatátvitel sebezhetősége

2.2.2.1 A vezetékmentes hálózatról általánosságban

Először néhány mondatban szeretnék kitérni a vezetékmentes hálózatok felépítéséről, hiszen a számítógépek fejlődésének köszönhetően jelent meg az igény erre a helytől független adateléréshez, valamint ez a technológia teszi lehetővé a kézi számítógépek mobil hálózati felhasználását. A vezeték nélküli megoldások előnye a kiépített vezetékes hálózattokkal szemben, hogy csupán kis mértékben függenek a kábelezés kiépítésétől. A legnagyobb előnyük ezeknek a megoldásoknak, hogy a felhasználók mobilitása nagymértékben megnövekedett, ezáltal is növelve a munkavégzés hatékonyságát és az adatok hordozhatóságát.

Az adatátvitel modulált rádióhullám segítségével történik. Az elméleti adatátviteli sebessége 11Mbps vagy 54Mbps, ami függ a helyszíni viszonyoktól, a titkosítás ki/bekapcsolásától.

3. ábra

Egy WLAN hálózat felépítése.

A WLAN rádiófrekvenciás eszközök az ISM (Industrial, Scientific, and Medicine) sávban működnek. Az ISM sávok a rádiófrekvenciás spektrum UHF illetve SHF tartományában helyezkednek el. A különböző gyártó cégek saját termékeikben saját technológiákat használtak, így az eszközök nem tudtak egymással kommunikálni. Igény

merült fel tehát egy szabvány kidolgozására és erre, akárcsak a vezetékes hálózatok szabványánál az IEEE[22]- t kérték fel.

A szabvány a 802.11-es elnevezést kapta, melyet rövidesen több másik változat is követett. A jelenlegi szabványok 802.11a, 802.11b, és 802.11g, valamint fejlesztés és bevezetés alatt áll a 802.11n, melyek a frekvencia tartományban és a sebességükben térnek el egymástól. A szabványt és a kompatibilitást betartó termékeket Wi-Fi címkével minősítik. A hétköznapi szóhasználatban a Wi-Fi - t gyakran azonosítják az IEEE 802.11- es család valamelyik tagjával, hasonlóan ahhoz, ahogyan a vezetékes hálózatok megnevezéseként a 802.3 helyett az Ethernet kifejezés terjedt el.

2.2.2.2 A vezetékmentes hálózatok fenyegetései

Léteznek olyan fenyegetések, amelyek kimondottan a vezeték nélküli hálózatokra jellemzőek. Ezek között vannak passzív módszerek, amikor a támadó nem avatkozik bele közvetlenül a kommunikációba, és vannak aktív támadási módszerek, amikor a támadás során az adatokhoz közvetlenül hozzáfér a támadást végrehajtó.

Egyik ilyen veszélyforrás, a **lehallgatás**. Ekkor egy harmadik fél jogosultság nélkül fér hozzá a vezetékmentes kommunikációban részt vevő üzenethez és nem szükséges közel férkőznie az adó vagy a vevő helyéhez. Egy, a küldés előtt titkosított üzenet alkalmazásával azonban biztosítható, hogy a lehallgatást végző fél ne legyen képes az eredeti üzenetet visszafejteni. A lehallgatást alkalmazva a hálózati kommunikáció elemzéséből akár a kapcsolat titkosításának feltöréséhez is lehet információhoz jutni.

Adatmódosításról beszélünk akkor, ha egy harmadik fél módosítani is képes a lehallgatás során ellopott üzenetet, vagy adatokat, és úgy küldi azokat tovább a címzettnek. Az ilyen támadást man-in-the-middle,[23] magyarul közbeékelődéses támadásnak hívják. Ezeken kívül létezik még az úgynevezett **megszemélyesítés**es támadás, amikor valaki hitelesített félnek adja ki magát jogosulatlanul, és úgy kapcsolódik a hálózathoz.

Mindezekből látszik, hogy a vezeték nélküli hálózatoknak a praktikusságában van kockázatuk, hiszen az információt rádiós úton továbbítják, ezáltal kevésbé

[22] **IEEE**: (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) Villamos- és Elektronikai Mérnökök Intézete. A szabványosítás világának egyik legfontosabb résztvevője, szabványokat dolgoz ki.

[23] A man-in-the-middle támadások célja a bizalmasság, integritás és a rendelkezésre állás meghiúsítása.

biztonságosak, hiszen könnyen lehallgathatóak. Az illetéktelen hozzáférések megakadályozásának elősegítése céljából a WLAN szabványok tartalmaznak különböző biztonsági protokollokat. Ezeket használva csökkenthető a vezetékmentes hálózat támadhatósága, ezért nézzük meg őket kicsit közelebbről:

WEP[24]

Ugyan már javítottak rajta, de könnyen feltörhető. Három fő funkcióját, mely szerint biztosítania kellene az átvitt információ védettségét, megakadályozni az illetéktelen belépést a vezeték nélküli hálózatba és védettséget kell biztosítania a módosított információ visszajuttatása ellen, nem tudja maradéktalanul teljesíteni.

WPA[25]

A hálózati kártyák és AP[26] - k frissítését követően egy szabványos és biztonságos megoldást kapunk. A szabvány kötelezővé teszi a gyakori kulcscserét, és bevezet egy új visszajátszás elleni védelmet. Jól skálázható megoldás nagy, közép vagy kisvállalati szinten is. A WPA egy köztes megoldás a WEP és a 802.11i szabvány között, amit WPA2 – ként neveznek.

WPA2[27]

A WPA2 szabvány a 802.11i szabványra épül, melynek szerves részét képezi a WPA. A WPA és WPA2 közötti különbség az erősebb kódolásban van, a WPA2 AES - t (Advanced Encryption Standard) használ a forgalom titkosítására, míg a WPA csak a TKIP - t (Temporal Key Integrity Protocol) nevezi meg titkosítási eljárásaként.

[24] **WEP**: **W**ired **E**quivalent **P**rivacy a kezdeti WiFi szabványok biztonsági technológiája, mára elavult.

[25] **WPA**: A **W**i-Fi **P**rotected **A**ccess a Wi-Fi hálózatok biztonságát szolgáló védelmi és azonosítási rendszer. A WEP gyengeségeinek orvoslására hozták létre.

[26] **AP**: **A**cces **P**oint. Olyan hálózati eszköz, mely interfészként szolgál vezeték nélküli kommunikációra alkalmas eszközök és a hálózat többi része közt.

[27]**WPA2**: Új titkosítási és biztonsági eljárásaival nagyobb biztonságot nyújt, mint a WEP vagy a WPA.

A WPA vagy WPA2 hálózatok esetében PSK vagyis Pre-shared key (előre megosztott kulcs) módban a hozzáféréshez szükséges biztonsági kulcsot minden felhasználónak egyszerűen csak be kell ütnie, hogy beléphessen a hálózatba. Ez a kód 8-tól 63 nyomtatott ASCII[28] karakterig terjedhet, vagy 64 hexadecimális szám lehet. A törése gyakorlatilag csak akkor valósítható meg, ha gyenge jelszót választ magának a felhasználó.

Amennyiben a kommunikáció titkosítás nélküli használatára kerül sor, akkor elég könnyű a behatolás, hiszen nincs szükség fizikai kapcsolatra. Fontos tehát egy vezeték nélküli hálózat alkalmazásakor, hogy odafigyeljünk a biztonságos kommunikációra. Alapállapotban a WiFi eszközök kevés biztonsági beállítást tartalmaznak, éppen ezért fontos, hogy soha ne hagyjunk semmit gyári beállításokon, főleg a gyári jelszót ne!

A PDA készülék vezetékmentes hálózati beállításai között (1 számú melléklet) lehetőségünk van a kiválasztott hálózat nevének, a csatlakozás típusának (rejtett, vagy sem) megtekintésére, megadására. A hálózati hitelesítés beállításánál kiválasztható a biztonsági protokollok közül az, ami szükséges a biztonságos hálózathoz való csatlakozáshoz.

2.2.2.3 A Bluetooth kapcsolat

Létezik egy másik vezeték nélküli adatátviteli protokoll a mobiltelefonok és a hozzá illeszthető perifériák közötti néhány méteres távolság áthidalására, ami kiváltja a berendezések összeköttetésére használt kábeleket. Ez a Bluetooth, amit 1994-ben közös munkával hozta létre az Ericsson, az IBM, az Intel, a Nokia, és a Toshiba.

Nevét a viking Harald Blaatandról – angol nevén Harald Bluetooth (Kékfogú Harald) – kapta, aki Norvégiát és Dániát egyesítette. A Bluetooth szabványt felismerő eszközök a 2400–2483.5 megahertz közötti hullámsávban egyszerre 8 darab, de legfeljebb 10 méteres körben megtalálható periféria kezelésére képesek. Az így elérhető elméleti adatátviteli sebesség 1 megabit/másodperc, de a sebesség elsősorban a gyakori rádiócsatorna váltások miatt a gyakorlatban nem haladja meg a 400–500 kbit/másodpercet. A Bluetooth hasonlóan a WLAN - okhoz a 2.4 GHz-es ISM sávban

[28] **ASCII**: (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) Egy amerikai szabványos információcsere-kódrendszer, amely a latin abc - n alapul.

működik. Ezt a technológiát, a mobil eszközökben (mobiltelefonok, PDA-k, notebookok, stb.) alkalmazzák a gyártók előszeretettel, ami egy könnyebben, gyorsabban létrehozható adatátvitelt létesít a kézi számítógépek és egyéb, a technológiát alkalmazó eszközök, úgymint a mobiltelefonok vagy - egy megfelelő kártya beszerelése után - az asztali számítógéphez csatlakoztatva. Maga a Bluetooth protokoll nem sérülékeny, a támadásokat eddig mindig a megvalósítás és a felhasználás hibáit kihasználva követik el.

A Bluetooth szabvány által alkalmazott rádiós hatótávolság csekély, ez pedig minimalizálja az elkövetés valószínűségét, hiszen majdnem „fizikai" közelségbe kell kerülni a készülékkel az elkövetéshez. Ráadásul a legtöbb támadáshoz pártosítani kell az eszközöket, amihez a felhasználók hozzájárulására van szükség. Létezik egy Bluezard nevű program, ami Windows Mobile és PocketPC - n futtatható. Ez egy komplett Bluetooth kezelő alkalmazás. Képes arra, hogy irányítsa a másik készüléket, valamint az úgynevezett „Bluesnarf" támadások végrehajtására, amelyeknek a lényege, hogy alkalmassá teszi a támadót a fájlrendszer tallózására, le- és feltöltésre, törlésre és mappák létrehozására. Ezen kívül többlet információkat is szolgáltat a megtámadott készülékekről (például a Bluetooth MAC[29] address) és képes felfedezni a láthatatlan eszközöket is. Ennek a támadásnak a kivitelezéséhez azonban szükséges a felhasználó, vagyis az „áldozat" közreműködése, hiszen csak a párosítás elvégzése után válik támadhatóvá az adott készülék.

A védekezés a támadások ellen viszonylag egyszerű, csupán a Bluetooth használatának korlátozását kell szem előtt tartani. Kizárólag akkor engedélyezzük, amikor tényleg szükségünk van rá. A PIN kód használatánál pedig figyeljünk arra, hogy olyan hosszúságút válasszunk, amit nehezebb feltörni (6 – 8 karakter). Csak akkor fogadjunk el bármit a készülékünkre Bluetooth kapcsolaton keresztül, ha biztosan tudjuk, hogy kitől jön, és ha valóban szükségünk van rá.

[29] Egyedi hardware alapú azonosító kód, melyet egy hálózati kapcsolatban résztvevő felhasználók megkülönböztetésére használnak. Meg lehet őket hamisítani, illetve a hálózat résztvevői felé hamis MAC címet lehet mutatni.

2.3 Sebezhetőségek

2.3.1 Az adattárolás sebezhetősége

A különböző számítástechnikai eszközök, így a kézi számítógépek adattároló képessége folyamatos növekedésben van. Ma 100 gigabit információt el lehet már tárolni egyetlen négyzet inch (6,45 cm²) felületen. A kérdés csupán az, hogy a fontos adatokat hogyan, milyen módon tároljuk, és védjük. A korszerű kézi-számítógépek memóriakártya bővítési lehetőséggel rendelkeznek és ezek között manapság már nem ritka a 16-32 GB kapacitású sem. A nagyobb védelem érdekében nemcsak szükséges, hanem elengedhetetlen az adatok titkosítása, hiszen egyre több és kifinomultabb kockázat fenyegeti azok biztonságát. A célzott támadások nem kerülik el a tárolóeszközöket sem. Nyilvánvaló, hogy nem kell mindent titkosítani, de azon információkat, amelyek érzékenyek, bizalmasak, valamint védendő vagy személyes adatok, mindenképpen célszerű titkosítani. Hiába bombabiztos egy hálózat, vagy védelem, ha valakinek a kezébe kerül egy PDA tele fontos üzleti információkat tartalmazó titkosítás nélküli fájlokkal. Mára már számos olyan szoftveres és hardveres megoldás létezik, ami megfelelő biztonsággal képes megvédeni a mobil eszközök tároló elemein elhelyezkedő adatokat, lehetetlenné téve az eszközt megszerző számára, hogy a tárolt információhoz hozzáférjen. Ilyen termékeket számos cég kínál, ezek nem csak beágyazott Windows operációs rendszeren, de Symbian rendszeren is elérhetőek.

Egyes PDA - kon létezik a tároló kártyákra mentett fájlok tikosításának a lehetősége, ami azt jelenti, hogy az adott eszköz úgy menti el az adatokat, hogy a visszaolvasásra kizárólag csak ő képes, másik készülék, vagy személyi számítógép nem tudja elolvasni azokat. Ez a megoldás életképtelen egy olyan helyzetben, ahol az adatokat át kell vinni egyik gépről a másikra és nincs lehetőség a vezetékmentes hálózat, vagy Bluetooth használatára valamilyen okból.

Vannak olyan készülékek, amelyekből a memóriakártyát egyetlen mozdulattal el lehet távolítani, ezért idegen hozzáférés esetén nem nyújt kellő biztonságot az ilyen típusú készülékek használata. Fontos, hogy a kézi-számítógépeken tárolt adatokról megfelelő gyakorisággal biztonsági mentés készüljön. Az egyik legfontosabb dolog, ami nélkül nem működik a védelem, az a felhasználó hozzáállása, ezért oktatással tudatosítani kell benne, hogy milyen veszélynek vannak kitéve az adatai, ha mobil eszközt használ a munkája során illetve azt, hogy betartsa a tőle megkövetelt felhasználói előírásokat. Ezek között szerepelnie kell a rendszeres adatmentésnek a

fontossága, a nem engedélyezett programok telepítésének mellőzése, vagy a megfelelő biztonságú protokollok kizárólagos alkalmazása.

A tárolt adatainkra a legnagyobb kockázatot jelentő veszélyforrások a következők:

Megnevezés	Leírás
Illetéktelen hozzáférés	Az adott dokumentumhoz olyan személy vagy személyek férnek hozzá, akiknek a dokumentum kezelése nem feladata. Ilyenkor sérül a dokumentumok bizalmassága.
Téves adatkezelés	A dokumentumon végzett olyan művelet, vagy módosítás, aminek végrehajtására nincs szükség. Ebben az esetben az adatokat ismét elő kell állítani, beszerezni, vagy az utolsó hiteles állapotot elő kell állítani.
Véletlen törlés	Olyan dokumentumok kerülnek törlésre, amire később még szükség lenne. Ilyenkor az adatokat ismét elő kell állítani, be kell szerezni, az utolsó hiteles állapotot elő kell állítani.
Vírusfertőzés	A vírusok a számítógépen tárolt adatokat igen sokféleképpen károsíthatják, ezért egy vírusfertőzés esetén az okozott kár elég jelentős is lehet.
Műszaki meghibásodás	Olyan esetben, amikor hardveres hiba történik, az adatok nem elérhetőek, vagy olyan sérülés következik be, amitől akár végleg el is veszhetnek.
Tűz, természeti katasztrófa	Teljesen meg tudja semmisíteni nemcsak az adatokat, de a tárolására szolgáló kézi-számítógépet is.
Rosszindulat	A szándékosan ártani akaró cselekvést értem ez alatt, ami az adatok sértetlensége és rendelkezésre állása ellen irányul.

1. táblázat
A tárolt adatok kockázata.

2.3.2 Hozzáférési sebezhetőségek

A hozzáférés azt jelenti, hogy az informatikai eszközöket (jelen esetben a szakdolgozat tárgyát képező kézi-számítógépeket) csak a feladatából eredő indokolt esetben, és ellenőrizhető módon szabad mások által hozzáférhetővé tenni.

A következő hozzáférési típusokat lehet elkülöníteni:

- Fizikai hozzáférések (közvetlenül az eszközhöz)
- Logikai hozzáférések (a rajta tárolt adatokhoz, információhoz)

Általánosan elmondható, hogy csak a szükséges jogokat szabad kiadni, mely során figyelembe kell venni a biztonsággal kapcsolatos igényeket. A kézi-számítógépekkel kapcsolatos egyik cél az illetéktelen hozzáférések megakadályozása. Ehhez felhasználói

azonosításra van szükség. Elvesztés, vagy ellopás esetén az adatok támadhatóságát nagymértékben megkönnyíti, ha nincs megfelelő azonosító és hitelesítő eljárás alkalmazva az eszköz védelmére. Hozzáférés-védelmi eljárások nélkül a hálózatban történő munkavégzés nem garantálja, hogy csak a rendszerhez engedélyezett hozzáférések valósulhassanak meg. Az alkalmazásokhoz való illetéktelen hozzáférés megtörténhet egy lopott készülékkel is, ami megfelelően van konfigurálva a hálózathoz, és a rendszerből való kiesése után nem zárták ki a készüléket a rendszerből, vagy az azt használó személy hozzáférését nem kezelték, tiltották le megfelelően. Könnyen előfordulhat, hogy vezetékmentes hálózathoz csatlakozva adatokat lophat, vírust telepíthet a támadó az eltulajdonított, és nem megfelelő azonosítással védett kézi-számítógépről a hálózat bármely eszközére.

Éppen ezért, a kiosztott hozzáférési jogosultságokat rendszeresen felül kell vizsgálni és módosítani, ha szükséges.

2.3.3 A trójai programok, a PortScan - erek, a Keyloggerek

A trójai programok

Ezeket a programokat az angol nyelvben RAT – nek (patkánynak) hívják, ami a Remote Administration Tools (Távoli Adminisztrációs Eszköz) szavakból képzett mozaikszó.

Trójai programoknak olyan programokat nevezünk, amelyek azt színlelik, hogy valamilyen hasznos tevékenységet végeznek, ám eközben a háttérben megbújik egy romboló programrészük is, amely titokban végzi áldatlan tevékenységét. A trójai programok felépítésüket tekintve két részből állnak. Van egy kiszolgáló rész, ami lényegesen kisebb méretű, ezt hívjuk szervernek és van egy méretileg nagyobb, ami az ügyfélrésze, ez pedig a kliens. Általában az operációs rendszer futása közben nem lehet törölni őket, mert alkalmazásban vannak. Ezek a programok hálózatos, internetes kapcsolat útján terjednek leginkább.

A trójai programok egy részében már beépített funkció, hogy a szerver futtatása után automatikusan küld egy e-mail üzenetet az áldozat IP[30] címe és egyéb fontos információval együtt, valamint, hogy sikeresen beírta magát a rendszerbe és rezidensé

[30] Az **IP**-cím (**I**nternet **P**rotocol) egy egyedi hálózati azonosító, amelyet az egymással kommunikáló számítógépek egymás azonosítására használnak.

vált. Ha megvan a cél IP címe, akkor a trójai kliensrészből kapcsolódva rá, képes a támadó adatokat törölni, fel-le tölteni, a gépet kikapcsolni, a futó programokat leállítani és elindítani, jelszavakat lopni, FTP[31] kapcsolatot használni. Mindezek csak töredékei annak, amit a támadó végrehajtani képes a trójai programok segítségével.

Hogyan is működnek ezek a programok?

Amikor a gépen fut a trójai szerver része, akkor egy portot nyit meg, amire bárki felcsatlakozhat, aki rendelkezik a kliens résszel. Természetesen a porton keresztül a trójai szerver részhez csatlakozik és vele kommunikál, nem pedig közvetlenül a géppel, vagyis csak azokat az utasításokat lehet kiadni, amiket a trójai program tartalmaz. Az áldozat gépén a trójai úgy viselkedik, mint egy vírus. Beírhatja magát a Windows könyvtárban található win.ini illetve system.ini fájlban vagy pedig a Windows regisztrációs adatbázisába. Egy profi támadás következtében szinte minden fontos személyes információt meg lehet szerezni, ami csak a számítógépen van.

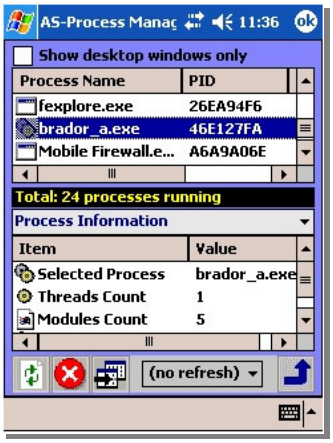
Ilyenek például:

Azonosítók és kódok	Vállalati azonosítók
Személyes címek és adatok	Családi képek
E-mail fiókok	Telefonszámok
E-mail levelek	Bankkártya információk

Az első ilyen jellegű kártevő, ami Windows CE – t futtató PDA - ra készült a Kaspersky Labs által felfedezett „Backdoor.WinCE.Brador.a” nevű, hátsó ajtót nyitó program. Azzal a céllal készült, hogy a készítő számára teljes hozzáférést biztosítson a fertőzött PDA - hoz a trójai program által megnyitott porton keresztül. Miután elindult, létrehoz egy „svchost.exe” - nevű fájlt a Windows autorun mappájában, ezáltal teljes körű hozzáférést szerez a rendszer fölött minden alkalommal, amikor a kézi számítógép bekapcsolt állapotban van. A Brador ezután azonosítja a gép IP-címét és azt elküldi egy üzenettel együtt, amiben tájékoztatja a készítőjét, hogy az eszköz csatlakozik az Internethez és a hátsó ajtó aktív. Végül a Brador megnyitja a 2989-et portot és várja a parancsokat. Programja szerint fájlokat tölt le és fel az eszközre, és számos további parancsot futtat. A többi hátsó ajtó típusú programhoz hasonlóan a Brador nem képes

[31] **FTP**: (**F**ile **T**ransver **P**rotocol) egy általánosan elterjedt kommunikációs protokoll a file - ok átvitelére bármely TCP/IP alapú hálózaton.

önállóan terjedni, érkezhet e-mail üzenethez csatolva, letölthető az internetről vagy asztali számítógépről más adatokkal együtt feltölthető a PDA - ra.



4. ábra
A Brador futás közben.

Egyre újabb, jobb, nagyobb funkcionalitással bíró, jobban rejtőzködni képes trójai programok készülnek.

PortScan

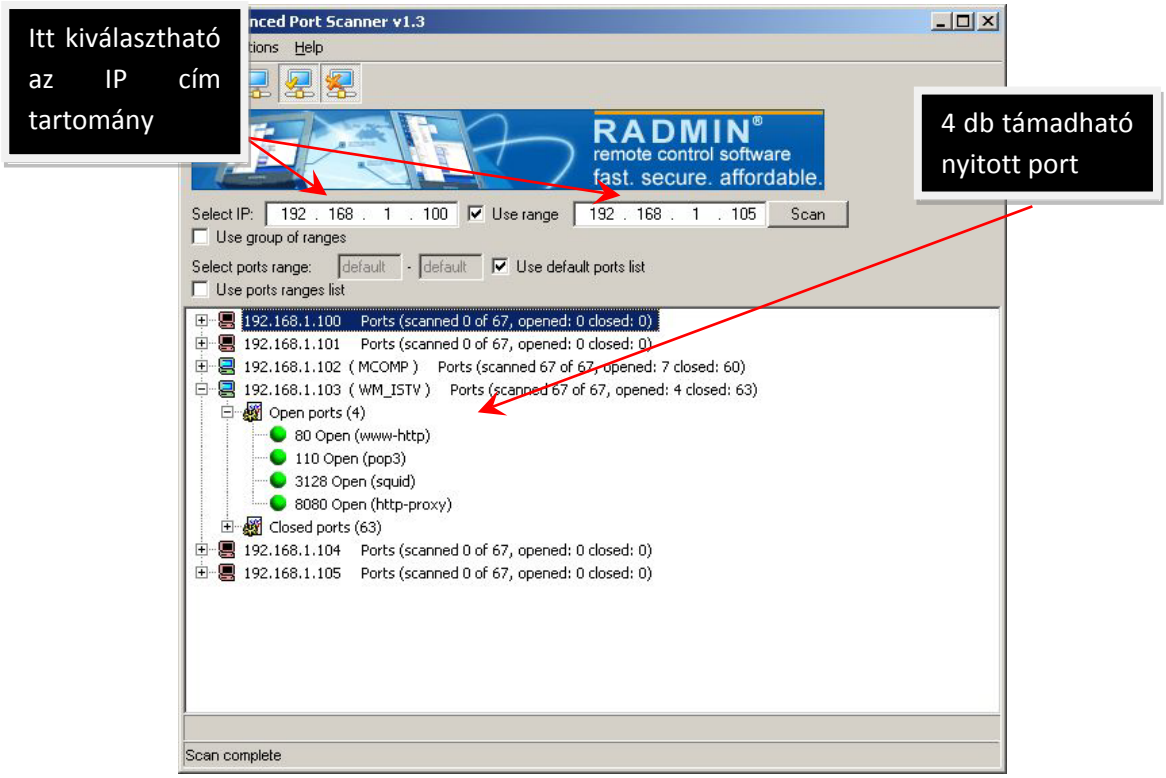
Az első, hálózati pásztázásra alkalmas eszköz, „ping" - névvel 1983 decemberében született. A hálózatbiztonsági pásztázások károkozásra alkalmas célja az információszerzés, a kritikus pontok megtalálása egy hálózatban.

Egy PortScan programmal végrehajtandó támadás elsőként megkeresi azokat az IP címeket, melyek a választott címtartományban elérhetőek (5. ábra), majd a célgép hálózati címére küldve egy próbacsomagot, válaszra vár. A válasz elmaradása egyet jelent azzal, hogy a célgép nem érhető el. A port scanner feladata, hogy a célgép egyenként 65535 TCP[32] és UDP[33] portja közül megkeresse azokat, amelyeket a gépen futó valamelyik alkalmazás nyitva tart. A működés alapvetően az, hogy az ellenőrző gép kapcsolatot próbál kezdeményezni a célgép adott portján át. Miután sikerrel jár, tudja, hogy a célgép valamilyen szolgáltatást nyújt azon az adott porton keresztül.

[32] **TCP**: (**T**ransmission **C**ontrol **P**rotocol) Az IP és az alkalmazás réteg között helyezkedik el, és ő felel az adatcsomagok hibamentes átviteléért és eredeti sorrendbe való visszaállításáért.

[33] **UDP**: (**U**ser **D**atagram **P**rotocol) Az Interneten alkalmazott TCP/IP protokollcsomag nem-megbízható, datagram típusú átvitelt biztosító tagja.

Az 5. ábrán az ASUS MYPAL A696 – os kézi számítógép nyitott portjait tekinthetjük meg (zöld színnel kiemelten) az internetkapcsolat ideje alatt.



5. ábra
Nyitott portok egy készüléken.

További funkció lehet egy PortScan programban, hogy képes nagy valószínűséggel megmondani, hogy milyen operációs rendszer fut a távoli gépen. A PortScan önmagában még nem okoz problémát, de könnyen lehet egy támadás első lépése.

Keylogger

A keylogger magyarul billentyűzetfigyelő a felhasználó által leütött billentyűket loggolja, azaz eltárolja a billentyűzet által közölt adatokat egy fájlba. Létezik olyan verziója is, amelyik a programok indítását és a kilépéseket is rögzíti. Nem számít vírusnak, mint a trójaiak, de egy trójai program tartalmazhatja a keyloggert, mint funkciót. Ezek is memóriarezidens programok.

A keylogging alkalmazásoknak jelenleg két csoportját különböztetjük meg	
A *szabad elérésű, általános célú* programok tartoznak az első csoportba, melyek ingyenesen letölthetők az internetről.	A *kimondottan támadási célú* keylogging programok a másik csoport. A rosszindulatú kódok által végrehajtott támadások részeként telepítődnek fel a kézi-számítógépekre.

2. táblázat
A Keylogging alkalmazások csoportosítása.

Igazából ezeket az alkalmazásokat a kereskedelmi vagy otthoni PC használat szándékolt nyomon követésére szánták, könnyedén felhasználhatók azonban rosszindulatú célokra.

2.3.4 Jelszófeltörés

Alapesetben a felhasználói azonosítóhoz olyan jelszót választunk, amelyet csak a rendszer és a jelszó tulajdonosa ismer. Így amikor be kíván lépni a rendszerbe, e két információ együttes megadásával igazolja azonosságát az illetékes felhasználó. A rendszer érzékeli, hogy az éppen beírt jelszó egyezik-e azzal, amelyet az adott felhasználói névre vonatkozóan tárol. Ha ez a két adat megegyezik, akkor lehetségessé válik a hozzáférés.

A jelszóalapú hitelesítés esetében az, aki tudja a jelszót, jogosult felhasználó, mivel olyan speciális ismerettel (mint a titkos jelszó) rendelkezik, amelyről senki másnak nem lehet tudomása. Ennek a megközelítésnek azonban megvan az a gyenge pontja, mely szerint lehetséges, hogy ugyanazt a jelszót többen tudják. Ez azért lehetséges, mert az ember alapvetően kényelmesebb annál, semhogy egy bonyolult jelszót megjegyezzen, ha az nem kötelessége. Ezért jól látható, könnyen elérhető helyre például felírja a jelszavát.

A jelszóalapú hitelesítés a jelszó *titkosságán* alapul, ezért a biztonság teljes mértékben a titoktartás mértékétől függ.

A legegyszerűbb módja annak, hogy egy jelszóval védett rendszert megtámadjanak az, hogy találomra különféle jelszavakkal próbálnak meg bejelentkezni. Az egyik legkézenfekvőbb, hogy a felhasználói azonosító és a jelszó megegyezik. Ezen kívül léteznek még a sablon szavak kategóriái (3. táblázat), amelyeket vagy azért választunk, mert a billentyűzeten való elrendezésüknek köszönhetően könnyen megjegyezhetők, vagy valamilyen szempontból az életünkhöz, mindennapjainkhoz köthetőek.

Az alábbi táblázatban összegyűjtöttem néhány tipikusan ebbe a kategóriába sorolható jelszavat:

A billentyűzet elrendezéséből adódó jelszavak	Az ember életéhez, mindennapokhoz köthető jelszavak
qwertz	A felhasználó neve, vagy beceneve
qwasyx	A házastárs, gyermek neve
asdf	A kedvenc háziállat neve
ayxasqw	Az saját autó forgalmiengedély-száma
jelszó	Az saját autó rendszáma
yxcv	A családon belüli születési dátumok
qwer	A házassági évforduló dátuma
0123	A telefonszámok

3. táblázat
A jelszavak kategóriái

A találgatásos támadások természetesen csak akkor működnek, ha a támadást végrehajtó fél tud valamit a célba vett felhasználóról. Ahogy korábban a Social Engineering fejezetben láttuk, ezekhez az információkhoz hozzá lehet jutni. A támadáshoz igénybe vehető még az interneten széles körben elérhető jelszó szótárak segítsége,[34] ahol sok különböző nyelven és különböző témákból listázott szó szerepel.

Ezen a módszeren túlmenően létezik még a különböző jelszó törő programok segítségét igénybe vevő támadás. Ezek az alkalmazások vagy egy adatbázisból, vagy egy programja szerinti generáló ciklusból keresi ki a különböző karakterkészletekből összeállított (betűk, számok, speciális karakterek) szavakat. Képes megtalálni és felfedni a jelszavakat nemcsak azon a számítógépen, amire feltelepült, hanem az összes hálózatra csatlakoztatott eszközön, így a kézi-számítógépeken is. Egy ilyen program a `LOphCrack`, de számos hasonló képességekkel megtervezett társa lelhető még fel az interneten.

A ma elterjedt jelszótörő programok keresési algoritmusa alapján kijelenthető, hogy nem nyújtanak kellő biztonságot azok a jelszó csoportok sem, amelyeket tisztán csak számok vagy szótári szavak alkotnak. Valamint a szótári szó + szám (a szó elején vagy

[34] Irodalom jegyzék: [21,22] hivatkozás.

végén), a szótári szó kis és nagybetűvel + szám (a szó elején vagy végén) összevonásából képzettek sem. (például: SzAvaY2009)

2.3.5 Az Operációs rendszer gyengesége

Korábban számos operációs rendszernél találkozhattunk alapértelmezés szerint installálva bizonyos (fiktív) felhasználói nevekkel és alapértelmezésű jelszóval. Ma már ezek szerencsére megváltoztak, de még számos alkalmazásnál felbukkannak az alapértelmezésű jelszavak és az ilyeneket változatlanul hagyva rendszerünket veszélynek tehetjük ki. A kézi számítógépek operációs rendszereit szerencsére elkerülték a komolyabb hibák, de néhány biztonsági rés így is felbukkanhat bennük. Ez alól kivétel az Ipohne, amely biztonsági szempontból a legsebezhetőbb. Gondoljunk csak bele, még a mostanában újdonságnak számító Iphone 3G jelszavas védelmét is meg lehet kerülni fizikai hozzáféréskor egy egyszerű billentyű kombináció alkalmazásával.

A Windows Mobile is szenvedett már a hibáktól, nála a szoftver böngészőjében fedezték fel, hogy néhány speciálisan formázott honlap meglátogatása memóriatúlcsordulást okozhat és lefagyasztja a készüléket. Ezen kívül a Microsoft új 6-os sorozatú rendszerében a Bluetooth eszközök nevének kezelésével kapcsolatos probléma szolgáltatásmegtagadás előidézésére használható fel. További információt[35] kaphatunk erről a http://milw0rm.com/exploits/6582 helyen.

Mint láthatjuk, a mobil készülékekbe gyártott operációs rendszerek sem teljesen biztonságosak, de egyszerűségüknek köszönhetően jóval kevesebb biztonsági hibával rendelkeznek, mint az asztali gépek operációs rendszerei.

[35] Irodalom jegyzék: [31] hivatkozás.

3. Fejezet

Miről szól ez a fejezet?

Ebben a fejezetben a PreDeCo – elvnek megfelelően kerül vizsgálatra a kézi-számítógép a következőképpen:

- Preventív: a támadások megelőzésére irányuló
- Detektív: a támadások felderítésére irányuló
- Korrektív: a támadások bekövetkezése utáni elhárításra irányuló eszközök, cselekmények bemutatása.

3.1 Preventív védelmi intézkedések.

A harmadik fejezet első részében a megelőzésre fordítható eszközök bemutatására és azok biztonságban betöltött szerepére helyezem a hangsúlyt.

Preventív védelmi intézkedéseken az olyan megelőző intézkedéseket értem, amelyek a lehető legjobban képesek megakadályozni a támadást és késleltetni annak következményeit. Kitérek a jelszavak kérdésére, a szoftverek naprakészen tartásának szükségességére, valamint az adatkapcsolat biztonságának fontosságára és a titkosítási eljárások bemutatására. Elemzésre kerül a hozzáférési jogosultság, és információvédelem kérdésköre csakúgy, mint a legfontosabb tényezőnek a felhasználónak a biztonságra gyakorolt hatása.

3.1.1 Jelszavak

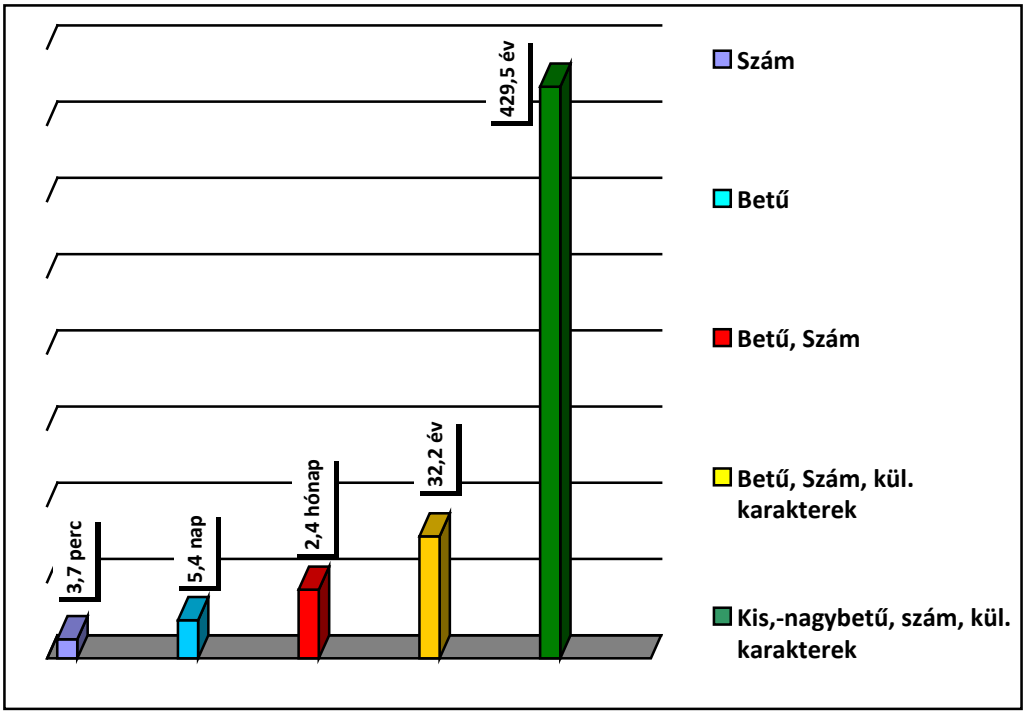
Mint azt az előző fejezetben láthattuk, a jelszavak kezelését korántsem lehet félvállról venni. Ahhoz, hogy a választott jelszó eleget tegyen a biztonság kritériumának - tehát képes legyen hatékonyan megvédeni a kézi-számítógépünket az illetéktelen felhasználástól - véleményem szerint az alábbi problémákat kell átgondolni:

- A legjobb jelszót nem lehet (nagyon nehéz) kitalálni.
- Ha a jelszót nem lehet kitalálni, valószínűleg nehéz megjegyezni.

- Ha a jelszót nehéz megjegyezni, a felhasználó feltehetően leírja valahová.
- Ha a jelszót leírják, az valószínűleg már nem biztonságos.

A jelszavak nagy részét a legtöbben tisztán csak számok, illetve kis, vagy nagybetűk kombinációk nélküli keverékéből képzik. Azonban ezeket a jelszófeltörő programok segítségével (lásd: 2.3.4 Jelszótörés fejezetrészt) viszonylag könnyen és elfogadható időn belül meg lehet fejteni. Az automatizált kereséssel átalakult, felgyorsult a jelszavak megfejtésére fordított munka/idő hányadosa.

Vizsgáljuk meg az alábbi diagramot (6. ábra):



6. ábra

A jelszó kombinációk feltöréséhez szükséges idő

Ebből kitűnik, hogy leggyorsabban megfejteni (~3,7 perc), a legkönnyebben megjegyezhető, csak a számok, vagy betűk felhasználásával létrehozott jelszavakat lehet. Míg a megfelelően megválasztott jelszavak megfejtése szinte lehetetlen.

A kézi-számítógépen tárolt adatok védelmében tehát olyan jelszavak alkalmazását célszerű megfontolni, amelyek elegendő védelmet nyújtanak a gyors megszerzésükre

irányuló kísérletek ellen. Ezek a 6-8 karakter hosszúságú kis és nagybetűk, valamint számok és a különleges karakterekből szerkesztett kódszavak használata.

Még jobban nehezíthetjük a támadást, ha bizonyos időközönként (3-6 havonta), cseréljük a jelszavakat és kis mértékben változtatjuk a hosszúságukat.

Hasznos módszer, és könnyen megjegyezhető, ha egy mondatból képezünk jelszót. Például: „ A kézi-számítógépek biztonsága elsődleges és lényeges! ” - mondatból megjegyezhető a „AkSZb1&L „jelszó. Ez az egyes szavak kezdőbetűiből és azok méretének ciklikus változtatásából, valamint ott ahol ez lehetőséget nyújt, a számok és különleges karakterek beépítésével felépített mozaikszó.

Összefoglalva tehát a helyes jelszóhasználatot a következőket lehet kijelenteni:

- Következetes jelszóválasztás, a könnyen kitalálható jelszavak mellőzése
- Titoktartás! (A jelszavak védelme)
- A jelszavak körültekintő tárolása (kódoltan, vagy sehogy)
- Az új jelszót nem célszerű az utolsó 5-10 régebbiből megalkotni
- A jelszavak rendszeres cseréje időközönként (háromhavonta, félévente)
- A jelszó kiderülésének gyanúja esetén újat kell létrehozni

Betartva ezeket az ajánlott lépéseket, sokkal közelebb kerülhetünk az ideális biztonsághoz.

3.1.2 Biztonságos szoftverfutási környezet

A biztonságos szoftverfutási környezet egy számítógépes rendszer biztonságának a legalapvetőbb eleme. A definícióját a következőképpen lehet megfogalmazni:

„A biztonságos futási környezet a számítógépes rendszer védelmi mechanizmusainak összessége, amely magába foglalja a hardvert, a firmware[36]-t és a szoftvert."

A szoftverek állapota azért fontos, mert egy elmaradt frissítés hibáit kihasználva akár támadhatóvá válik az eszköz. Habár folyamatos a kézi-számítógépeken futó operációs rendszerek fejlődése, mégis meglepő, milyen keveset törődnek a biztonságos környezettel. A jelenleg legújabb Microsoft Windows Mobile 6.1 Professional egyszerűsített operációs rendszer adatlapjából[37] például világosan kiderül, hogy a megannyi kényelembővítő szolgáltatás mellett csupán két új módosítás szolgálja a biztonság növelését (azok is csupán a Windows Mobile 6 - tól):

- Windows frissítés kezelő (működőképes!)
- Memóriakártya védelem

A szoftverfrissítések tartalmazhatnak rendszerhiba javításokat, különböző gyorsjavításokat, biztonsági frissítéseket és fontos szervizcsomagokat. Természetesen az operációs rendszeren kívül egyéb programok is megtalálhatóak a kézi-számítógépeken. Ezek mindegyikéhez használatuktól függetlenül - szolgáljanak akár a munkavégzés, akár a szórakozás céljából - tartoznak valamilyen frissítések, amelyek telepítését érdemes következetesen végrehajtani.

Napjainkban erre pedig már kényelmes lehetőséget biztosít az interneten keresztül történő, úgynevezett „élő frissítés" a gyártó honlapjáról, vagy akár a készüléken futó program beágyazott megoldásának használatával.

[36] A firmware egy olyan (néhány eszköz esetében frissíthető) program, mely az adott hardware eszköz belső vezérléséről gondoskodik.

[37] Irodalom jegyzék: [25,26] hivatkozás.

3.1.3 Adat és kommunikációs kapcsolat

A kézi-számítógépek legkönnyebben vezeték nélkül tudnak csatlakozni az informatikai környezethez. Ebből kézenfekvő, hogy a kialakított adatátviteli hálózatba történő belépéssel, a támadó közel tud kerülni a tárolt adatokhoz. Ilyen helyzetben természetesen mindenekelőtt a lehallgatás merül fel, a lehallgatással azután értékes információkhoz, pl. jelszavakhoz lehet jutni.

A kapcsolatban egy illetéktelen harmadik fél ellen leghatékonyabban a titkosított kommunikációval tudunk védekezni. A hálózatok kapcsolattitkosító eljárásainak mélyebb tanulmányozására eme szakdolgozat keretei nem adnak elég teret, de a vezetékmentes hálózat tikosításának lehetőségei megtalálhatóak a „A vezetékmentes hálózatok fenyegetései” (2.2.2.2) című fejezetrészben.

A kézi-számítógéppel adat kapcsolatot építő felhasználó különböző jogosultságokat kap a rendszer használatával, az erőforrásokhoz történő hozzáférésekkel kapcsolatban. Ezért valamilyen módon hitelesítenie kell magát, hogy csak azokat a jogosultságokat kapja meg, amelyek neki járnak. Ez egy három lépésben végrehajtott folyamat, melyben első lépésként a használatot kezdeményező fél azonosítót küld magáról a rendszernek. A következő lépésben a rendszer hitelesíti a kezdeményező felet, azaz a kapott azonosítót összeveti a rendszerben tárolt azonosítókkal. Ha egyezést talál, akkor harmadik lépésként a kezdeményezőt feljogosítja a hozzáférési joggal, hogy a hitelesítés megtörténhessen, és az illetéktelen hozzáférés kizárható legyen.

Létezik egy olyan lehetőség a kézi-számítógépek kommunikációs kapcsolatában (is), amely azt biztosítja, hogy egymástól távol eső számítógépek biztonságosan kommunikálhassanak egymással olyan nyilvános hálózaton – tipikusan az Interneten – keresztül, amely nem megbízható, vagyis adatbiztonsági szempontból nem tekinthető biztonságosnak. Ebben a kapcsolatban az adatbiztonságot nem az átviteli eszköz, hanem a titkosítás biztosítja.

Ez a Virtual Private Network vagyis Virtuális magánhálózat (a továbbiakban: VPN).

A VPN kapcsolattal olyan zárt közösségű hálózat hozható létre az Interneten belül, amelyet illetéktelenek nem használhatnak. Hatékony, biztonságos kommunikációs csatorna építhető fel általa, valamint olcsó megoldás.

Egy VPN kialakítása leegyszerűsítve azt jelenti, hogy minden egyes összekapcsolni kívánt hálózatrész és a nyilvános hálózat közé biztonsági átjárókat helyeznek el. Az

átjárók titkosítják a privát hálózatot elhagyó adatcsomagokat (kimenő forgalom), illetve dekódolják a nyilvános hálózatból érkező adatcsomagokat (bejövő forgalom), ezzel titkosított csatornát alakítva ki a nyilvános hálózaton. Ettől fogva a hálózatrész úgy viselkedik, mintha egyetlen nagyméretű privát hálózatot képezne.

Alapvetően három féle VPN típus létezik:

- Hardware közeli megoldások
- Tűzfal alapú megoldások
- Software közeli megoldások

A VPN tipikus alkalmazása, amikor egy munkatárs távolról kívánja elérni cége szerverét (pl. üzletkötői rendelésfelvétel), így a felhasználó számára a kapcsolat úgy jelenik meg, mintha közvetlenül a cége belső hálózatához csatlakozott volna.

3.1.4 Titkosító eljárások

Megvizsgálva a kézi-számítógépeken tárolt adatok típusait, elmondható, hogy főként kapcsolati információkat, illetve a kommunikációs folyamat eredményeként létrejövő dokumentumokat (pl.: e-mail vagy SMS, MMS, telefonszámok, amennyiben kombó a készülék) tárolnak el. Emellett azok az internet böngészőben eltárolt adatok is megjelennek az eszközön, amelyek egy vállalat információs rendszeréhez való csatlakozásához szükségesek. Az egyre nagyobb kapacitással rendelkező memória kártyák terjedése is elősegíti a rajtuk elhelyezett adatmennyiség növekedését.

A mobil eszközök támadhatósága elsősorban a fizikai eltulajdonításuk révén valósul meg. Így a bennük tárolt adatok megfelelő előzetes védelem nélkül, a támadó számára teljesen hozzáférhetőek. A külső memória kártya bővíthetőség is sérülékeny pontjuk, hiszen a legtöbb készülékből egy mozdulattal eltávolíthatóak, így, ha a tárolt adatokról nem készítettek biztonsági másolatot, akkor azok elvesztése is problémát okoz.

A később tárgyalt hozzáférés szabályozásával meggátolható, hogy egy támadó használni tudja a készüléket, az viszont nem akadályozható meg, hogy ha azt sikeresen kijátssza, akkor a háttértárolón elhelyezkedő adatokhoz szabadon hozzáférjen. Ezért van szükség a tárolt adatok titkosított védelmére. Ez történhet hardveres és szoftveres megoldással. A hardveres titkosítás előnye, hogy alkalmazás-függetlenséget biztosít. A

titkosítási folyamat a tárolóeszköz belsejében zajlik le, vagyis csak fizikai sérülés okozásával lehet hozzáférni az eszközön tárolt adatokhoz. Léteik azonban olyan hardveres védelem is, ami érzékeli, hogyha fizikailag akarják megkerülni, és ha van rá mód, az adatokat tönkre teszi. Ilyen megoldásról tájékozódhatunk a GORE – cég honlapjáról.[38]

Szoftveres titkosítást rengeteg cég kínál, számos változatban az interneten.[39] Ezek tudása sok esetben elegendő védelmet biztosít, melyek kiterjednek:

- PIM adatbázis védelmére (naptár, kapcsolatok, feladatok, e-mailek/SMS-ek)
- Fájlok titkosítása a lokális RAM-ban, és flash memóriában
- A titkosítási kulcsok generálására a jelszóból, ami megnehezíti a jelszó kitalálásán alapuló támadásokat.

A külső biztonsági programok alkalmazása mellett a támadó számára lehetetlen vagy nehéz az eszközökön tárolt adatokhoz való hozzáférés.

3.1.5 A felhasználó személye (Az ember, mint gyenge láncszem)

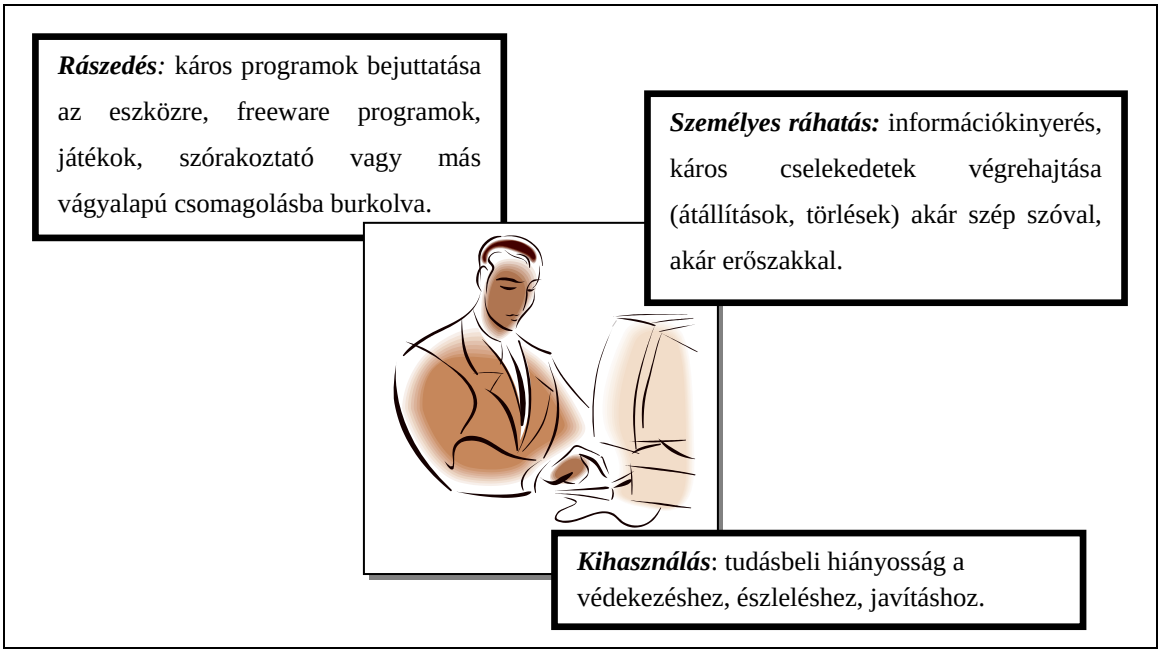
Minden technikai, szervezeti és szabályzati eszközök, módszerek és eljárások kitalálója, bevezetője, fenntartója és kihágója az ember. Az ember által elkövethető leggyakoribb hibák a frissítések, mentések elhanyagolása (hiányzik; egyáltalán nem, vagy nem biztonságosan tárolt) és a téves bizalom (Social Engineering) megléte. Nem is gondolnánk, hogy mekkora támadási felületet nyújtanak a jóhiszemű felhasználók, akik egy magát rendszergazdának kiadó személy felkérésére hajlandók gépeikre ismeretlen eredetű programokat telepíteni, vagy jelszavakat és egyéb érzékeny információkat kiadni. A jóindulatú támadás egyfajta “user scanner” - ként a felhasználók körében fellelhető emberi természetből eredő biztonsági hiányosságokra próbál rátalálni és ráhatni.

(A felhasználó érzékenysége a különféle támadásokra a 2.2.1 Social Engineering fejezetrészben bővebben kifejtésre került.)

A 7. ábrán a három legjellemzőbb emberi sebezhetőség fedezhető fel:

[38] Irodalom jegyzék: [27] hivatkozás.

[39] Irodalom jegyzék: [28] hivatkozás.



7. ábra
Az emberi láncszem gyengeségei.

Mindegyik orvosolható megfelelő szintű oktatással, mégis a legtöbb probléma sokszor a felhasználók nem megfelelő felkészítéséből, valamint az eszköz helytelen használatból származik. Egy felkészítésének magába kell foglalnia a munkavégzéshez szükséges teendők és eszközök ismeretét. Amennyiben a munkakör megkívánja, akkor a különleges (netán addig még soha elő nem fordult) esetek megismerését és lehetséges kezelését is tartalmazhatja. Esetleg már a munkaerő felvételnél kitűzhető szempont lehet, hogy a leendő alkalmazottnak legyen érzékenysége a gyanús esetek kiszűréséhez, mert előfordulhat, hogy még az előzetes felhívás sem elégséges a személyes ráhatás kivédéséhez. Ezek különösen fontos dolgok, hiszen a kézi-számítógépek kis méretüknél és mobilitásuknál fogva jóval nagyobb veszélynek vannak kitéve, mint az asztali számítógép, ami helyhez kötött, nehezen mozgatható, ezáltal például az eltulajdonítása sokkal nehezebben kivitelezhető, mint egy PDA – készüléké.

A felhasználók mindegyike az oktatás ellenére sem fog jobban odafigyelni a biztonságra, ezért létrehozhatóak különféle egyszerű szabályok, amiket kötelezően alkalmazni és maradéktalan betartását folyamatosan ellenőrizni kell. Ezek lehetnek:

- Az eszköz tárolására vonatkozó (munkahelyen, vagy azon kívül),
- Az eszközön tárolt adatokra vonatkozó (miket lehet, miket tilos),

- A felhasználó felelősségének tisztázására vonatkozó szabályok.

A kártékony programok is arra építenek, hogy a felhasználók még a sorozatos biztonsági figyelmeztetések ellenére is, saját maguk telepítik fel őket a készülékükre.

Figyeljük meg a 4. táblázatban, hogy az ember által elkövethető támadások besorolására, az informatikai biztonság osztályozási szempontrendszere szerint milyen csoportosítás állítható fel:

Elkövetés módja lehet	Elkövetés jellege lehet
Szándék szerinti	tudatos, vétlen
Jogállás szerinti	felnőtt, fiatalkorú, külsős, belsős, idegen
Tudás szerinti	profi, amatőr
Cél szerinti	károkozó, információt lopó, lejárató
Eszköz szerinti	saját fejlesztésű, nyilvánosan elérhető, automatikus

4. táblázat
Az ember által elkövethető támadások besorolása.

Sokan megengedik a barátok, családtagok és kollégáik számára, hogy hozzáférjenek a PDA – juhoz, internetezzenek, játékokat futassanak rajta, esetleg e-mailjüket megnézhessék. Még akkor is, ha a végletekig a bizalmat élvezi az, akinek a kezébe kerül a készülék, bizony megeshet önhibáján kívül, hogy ártó szándékú alkalmazást telepít, vagy adatot töröl.

3.1.6 Hozzáférés, jogosultság (Autentikáció, Autorizáció)

A hozzáférés és jogosultság kezelés célja megvédeni az információt a jogosulatlan hozzáféréstől, valamint az illetéktelen beavatkozástól. A két fogalom által rejtett taralom szorosan kapcsolódik egymáshoz, és ez a kapcsolat az egymáshoz viszonyított sorrendiségben is meghatározott, többnyire az *autentikáció* megelőzi az *autorizációt*.

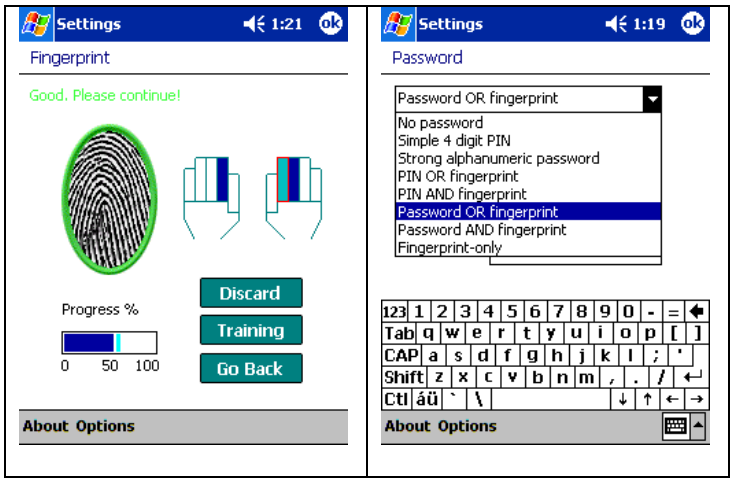
A felhasználó-azonosítás minden informatikai biztonsági rendszer alapja, ezért a kézi-számítógépek biztonságának tárgyalásakor sem lehet mellőzni. Az ***autentikáció*** olyan folyamat, amely arra szolgál, hogy valaki bizonyítsa az önmagáról állítottak valódiságát. Nagyon fontos az eszközökhöz való megfelelő szintű hozzáférés szabályozása valamilyen felhasználó-azonosítási módszerrel, ami lehet birtok-, tudás-, vagy biometriai alapú. Ezáltal az illetéktelen fél nem veheti igénybe a kézi-számítógép szolgáltatásait, nem juthat értékes adatok birtokába.

- A **tudásalapú** azonosítás a felhasználó birtokában lévő tudásra épül, arra, hogy a felhasználó *mit tud*.

- A **birtokalapú** azonosítás a felhasználó birtokában lévő tárgyra épül, vagyis arra, hogy a felhasználónak *mije van*.

- A **biometria alapú** azonosítás a felhasználó valamilyen tulajdonságára épít, közvetlenül azt vizsgálja, hogy a felhasználó fizikai-biológiai voltában *kicsoda*.

Az első PDA, amelyiknél alkalmazták a biometrikus azonosítást, az iPAQ h5450 volt 2002 novemberében. A legpontosabb választ a biometria adja arra, hogy valaki valóban az-e, akinek állítja magát. A biometria az egyént azonosítja, de fontos kiemelni, hogy ez sem ad tökéletes és minden körülmény között alkalmazható megoldást.



8. ábra
Biometriai azonosító szoftver futása egy PDA-n.

A három autentikációs módszer közül kettőnek az egymástól független, egyidejű kombinációja nyújtja a biztonságos azonosításhoz szükségesen ajánlott megoldást.

Az alkalmazott módszereket használhatóságuk, áruk és gyengeségeik alapján rendezhetjük csoportokba:

Csoportok	Tudás, avagy jelszó alapú azonosítás	Birtok, avagy kulcs alapú azonosítás	Biometrián alapuló azonosítás
Használhatósága	Használata egyszerű.	Használata általában egyszerű.	Egyes esetekben nehézkes, de megfelelő megvalósítás esetén nagyon megbízható.
Megvalósítás ára	Olcsó	Az olcsótól a drágáig	A komoly

		terjed az árskála.	megvalósítások drágák.
Gyengeségeik	Igazán erős védelmet jelentő jelszavak megjegyzése az ember számára nehéz.	Védekezni kell a másolás ellen (lehetőség szerint ne lehessen titokban másolni a kulcsot, mert ekkor az eltulajdonítás ténye nem vehető észre, és hosszabb ideig vissza lehet élni a másolat kulccsal).	Jogi, adatvédelmi (például biometrikus adatok tárolásának helye, módja) és egészségügyi (higiénia) problémái is lehetnek.
Megjegyzés	A tudás észrevétlenül másolható és tulajdonítható el (pl. nincs visszajelzés, arról, hogy valaki más is a jelszó birtokába jutott).	Eltulajdonítható (bár az eltulajdonítás ténye érzékelhető, a kulcs letiltható).	Egyszerű megvalósítások általában könnyen kijátszhatóak.

5. táblázat
A felhasználó-azonosítás csoportosítása.

A jelszavas azonosítás ma már valamennyi készüléken elérhető. A legújabbaknál pedig már kiküszöbölték azt a problémát, ami abból adódott, hogy az eszköz bekapcsolásakor a jelszavas védelme kijátszható volt egy Hard Reset[40]-el. Ennek az újraindításnak a következménye, a készüléken tárolt összes adat file, vagy program törlődése (a ROM-ban tároltakat kivéve), miközben a készülék minden beállítása visszaáll a gyári alapállapotra. Így kitörölhetők voltak a ROM-ból a jelszó beállítások, majd az újraindulást követően már nem kérte a jelszavas azonosítást. Némely operációs rendszeren a bejelentkezési jelszóként használt egyszerű PIN csak számokból álló jelszót jelent, amit egy jelszó emlékeztető mondattal lehet kiegészíteni.

A tudás alapú autentikációs rendszerek többnyire az operációs rendszer részei. Ezen kívül léteznek olyanok, amik az adott operációs rendszerre telepíthetőek és általában bővített szolgáltatás csomaggal rendelkeznek, így nagyobb biztonságot nyújthatnak az erősebb és skálázható erősségű titkosítással, és az olyan kiegészítő megoldásokkal, mint pl. a háttértároló titkosítása. Ebben az esetben a sikeres bejelentkezést követően a

[40] A Hard Reset az operációs rendszer, a meghajtó programok, valamint a gyakran használt alkalmazások újratelepítését jelenti. Ez többnyire egy billentyűzet kombináció, és a Reset gomb együttes alkalmazásával érhető el a készülékeken.

felhasználó számára használhatóvá válik a háttértár, míg a sikertelen autentikáció után a háttértár olvashatatlan lesz, mert titkosított marad akkor is, ha fizikailag hozzáférnek a háttértárolóhoz a támadók. Előnye a bizalmasság magas foka, hátránya, hogy amennyiben a felhasználó sem tudja magát igazolni, úgy ő sem fér hozzá a háttértárhoz.

Az ***autorizáció*** azon jogok megadása amelyekkel - az erőforrásokkal és adatokkal kapcsolatban - előre meghatározott szabályok szerint rendelkezhetnek.

A ma használatos PDA operációs rendszerekben egy adott mappát csak olvashatóvá, illetve rejtetté tudjuk tenni, viszont nem tudunk felhasználói jogosultságokat kezelni, hozzárendelni. A sikeres bejelentkezést követően bárki vissza tudja állítani a mappa láthatóságát, és módosíthatóságát. Emiatt itt is érvényes az, ami az autentikációnál, vagyis a jogosultságok kezelésére az operációs rendszerek is adnak ugyan támogatást, de a nagyobb biztonságot az erre a célra kifejlesztett alkalmazások használatával tudunk csak elérni. Ezek már képesek rá, hogy

- Konfigurálható felhasználói, biztonsági beállítások, titkosítási- és jelszó szabályokat
- Konfigurálható rendszergazdai jogokat csoportok, vagy egyének számára hozzanak létre és kezeljenek.

Például a Microsoft operációs rendszere a Windows Mobile ma már teljes egészében beilleszthető a vállalati informatikai infrastruktúrába. A Microsoft rendszerfelügyeleti megoldásának köszönhetően (Mobile Device Manager 2008) a készülékeken már egészen aprólékos szinten lehet kezelni a szoftverfrissítéseket, letiltható vagy engedélyezhető a Bluetoothkapcsolat, és titkosíthatóvá válik a memóriakártya.

Szükségesnek látom, hogy beszéljek arról, hogyan kell kezelni azokat az eseteket, amikor elszámolási kötelezettséggel járó, munkaeszközként kézi-számítógépet használó alkalmazott munkaviszonyába történik változás.

A munkaviszony megszüntetésekor biztonsági alapkövetelmény, hogy az alkalmazott, rendezett módon szolgáltassa vissza az általa használt kézi-számítógépet, illetve a rajta tárolt információkat, nehogy azokkal a későbbiekben bosszúvágyból vissza tudjon élni. Az általa ismert jelszavak cseréjéről gondoskodni kell. A felmondás alatt álló sértődött személy a biztonsági előírásokkal már nem sokat törődve az általa addig jogosultan elért információkat gyűjtheti a későbbi rosszindulatú felhasználás céljából. Éppen ezért egy távozó munkatárs szinte minden esetben biztonsági kockázatot jelent.

Abban az esetben, amikor eladásra kerül egy ilyen készülék, akkor az eszközről az arra jogosult és képzett személy minden, a szervezetet érintő adat biztonságos eltávolításáról kell, hogy gondoskodjon.

Biztonsági szempontból célszerű az alkalmazottakat informálni a személyzeti változásokról, elkerülendő egy adatszerzésre irányuló Social Engineering támadás a távozó munkatárs részéről a kollégái tájékozatlanságát és jóhiszeműségét kihasználva.

Amennyiben a felhasználónak a hozzáférési jogosultságai megmaradnak munkaviszonyának megszűnése, vagy munkakörének megváltozása után, és a készüléket nem szolgáltatta vissza, akkor már jogosulatlanul fér hozzá adatokhoz, így sérülhet az osztott biztonság elve, mely szerint az ideális állapot az, hogy minden munkatárs annyi információhoz férjen hozzá, amely a munkájához feltétlen szükséges. A kiosztott hozzáférési jogosultságokat minden felhasználó esetében időközönként felülvizsgálni és módosítani kell, ha a biztonsági igények megváltoztak.

3.1.7 Adatvédelem, információvédelem

Ezeknek a fogalmaknak a hallatán az emberek többségében téves elképzelések rajzolódnak ki, mert pontosan nincs a szemük előtt a fogalom kézzel fogható tárgya.

Tegyük fel tehát a kérdést, hogy mi is az információ?

Az információ fogalmának rengeteg megközelítése létezik attól függően, milyen tudományágakban kerül meghatározásra. Informatikai értelemben az információ adatokból épül fel, az adatok pedig bitek[41] sorozatából. Elfogadhatjuk tehát, hogy az adat a közlés formája, valamilyen rögzített **információ**, mely mindig ismeretet hordoz.

Ezen értelmezés szerint a biztonság alanya az információ (konkrét esetben információk egy meghatározott köre).

Jelen esetben az információszolgáltatás alapját a készülék saját és a külső memóriamodulján megtalálható adatok képezik. A biztonságuk ezért kiemelten kezelendő. Az adatbiztonság és az adatvédelem fogalmát külön kell kezelni egymástól. Míg az ***adatvédelem*** az adatok *jogi* értelemben vett (törvényekkel, szabályzatokkal

[41] A bit az információ, az információt hordozó közlemény hosszának egyik alapegysége. A név a binary digit (bináris számjegy) kifejezésből származik.

való) védelmét, addig az ***adatbiztonság*** fogalma magát a *technikai* védelmet, közvetlenül az adatok, az információk biztonságát jelenti.

A számítógépes rendszerek és a bennük eltárolt információk biztonságát informatikai biztonságnak nevezzük. Ennek két nagy területe, az ***információvédelem*** és a megbízható működés.

Az információ olyan értéket jelent, amelyet védeni kell a különböző fenyegetések ellen. Mindig szem előtt kell tartani, hogy az információt csak az arra jogosultak ismerhessék meg, az információ ne vesszen el (semmisüljön meg), illetve véletlenül, vagy jogosulatlanul ne módosuljon. Az információ három védendő tulajdonságát emeljük ki, ezek:

- Bizalmasság - **C**onfidentiality
- Sértetlenség - **I**ntegrity
- Rendelkezésre állás - **A**vailability

A felsorolt hármas követelményrendszert egyes dokumentumok angol betűrövidítéssel rendszerint– CIA – módszertannak nevezik.

3.1.7.1 Titkosság, bizalmasság (Secrecy, Confidentiality)

Ez a részterület foglalkozik az adatok illetéktelen kezekbe jutásának megakadályozásával. A hozzáférés-védelmi rendszerek és a rejtjelezési eljárások együttes használata biztosítja, hogy a magát igazoló fél a jogosultságának megfelelő mértékben kapjon hozzáférést. Ez biztosítja azt is, hogy kizárják az illetéktelen személy hozzáférését az adott információhoz (amennyiben a rejtjelkulcs titkossága biztosított).

A jogosultságok és hozzáférések megfelelő és következetes betartásával elérhető, hogy az illetéktelen személy csak irreálisan nagy erőbefektetéssel, költséggel, és igen kis valószínűséggel legyen képes a védett információhoz hozzájutni. A hitelesség erőssége abban rejlik, hogy két vagy több kommunikáló fél biztosan tudja azt, hogy azzal áll kapcsolatban, akivel szeretett volna és nem egy jogosulatlan harmadik féllel.

3.1.7.2 Sértetlenség (Integrity)

Egy információ, vagy rendszer sértetlenségéről akkor beszélünk, ha a kapott információról minden kétséget kizáróan megállapítható, hogy az előállítás óta változatlan maradt, vagy csak az arra jogosultsággal rendelkező változtatta meg.

A sértetlenség tekintetében az esetleges módosítás észlelésén és detektálásán van a hangsúly. Szorosan kapcsolódik hozzá az adat-konzisztencia, a hitelesség és letagadhatatlanság fogalma is. A sértetlenség a hozzáférés-védelmi rendszerek, illetve a titkosítás módszereinek (például ide tartozik a digitális aláírás is) alkalmazásával biztosítható, de ide sorolhatóak még a víruskeresés és egyéb védelmi megoldások széles tárháza is.

A sértetlenség elleni támadások kivitelezésénél a támadó nem csak a kommunikáció megfigyelésére, lehallgatására, hanem a cserélt információk módosítására is kísérletet tesz.

3.1.7.3 Rendelkezésre állás (Availability)

A rendelkezésre állásnál arról beszélünk, hogy egy rendszer, eszköz (esetünkben PDA), vagy az általa üzemeltetett szolgáltatás mennyi időre esik ki, vagy mennyi ideig látja el hibásan a feladatát. Röviden megfogalmazva a rendszer megbízhatóságát jelenti.

A rendelkezésre állás nem csak külső, rosszindulatú támadás esetén sérülhet. Figyelembe véve egy adott készülék körüli gyakorlati tényezőket láthatjuk, mennyi veszélynek van kitéve:

- Nem megfelelő üzemi hőmérséklet
- Szakszerűtlen karbantartás
- Szakszerűtlen használat
- Elemi károk (tűz, víz)
- Eltulajdonítás

3.2 Detektív védelmi intézkedések

Amint láttuk, a preventív védelemi kontrollnak az a lényege, hogy minél hamarabb észlelje egy nem kívánt esemény bekövetkezését, és korlátozza a káros hatás továbbterjedését az elhárító, helyreállító tevékenység minél hamarabbi megkezdéséig.

A detektív védelmi kontroll szerepe ezt követően az, hogy a bekövetkezett visszaéléseknél (pl. hálózati betörésnél, adat lopásnál) felismerje a támadás tényét és meggátolja, hogy a nem kívánt tevékenység kifejthesse hatását, és jelentősen nagy kárt okozzon.

3.2.1 Betörések felfedezése és kezelése

Amikor egy támadásnak sikerült kijátszani a megelőző védelmi eljárásokat, akkor még nem tekinthető sikeresnek, lezártnak. Voltaképpen akkor kezdődik az igazi kártevés, hiszen az adatokhoz hozzáférve elkezdődik azok szisztematikus kiválogatása, vagy teljes egészének a másolása. Ezen kívül a támadó különböző kódokat helyezhet el a cél eszközön, amik megbújva ott információkat gyűjthetnek, majd az internetre való csatlakozáskor kiszolgáltathatják azokat a számára. Ezek, természetesen nem történnek nyom nélkül, még egy kézi számítógép esetében sem. Ma már rengeteg eljárás, alkalmazás segíti a betörések felfedezését, és meggátolását a különböző asztali platformokon, de a PDA – k esetében még nem számíthatunk ilyen mértékű segítségre.

Éppen ezért fontos, hogy a készülék kezelőjének joga és kötelessége legyen, hogy az általa észlelt vagy tudomására jutott veszélyhelyzetnek (például időben nem javított biztonsági probléma) vagy betörésnek a mértékétől, annak várható következményeitől függően a megfelelő ideiglenes védekező lépéseket megtegye. Ezek:

- A készülék külső elérhetőségének a letiltása, ez lehet például az adott gépnek a hálózatról való eltávolítása, vagy más, az esetnek megfelelő mértékű intézkedés.
- A felhasználónak kötelessége legyen, hogy ha betörésgyanús esetet észlel, azt azonnal jelentse a cég biztonsági csoportjának, vagy személyes vezetőjének és a szükséges mértékben működjön együtt a károk elhárítása érdekében.

Példaként álljon itt néhány olyan jelenség, amelyek bekövetkezése esetén egy támadásra lehet gyanakodni:

- File-ok vagy könyvtárak között ismeretlen nevű bukkan fel,
- Korábban létezett file vagy könyvtár eltűnik,
- Egy file mérete ismert ok nélkül megváltozik,
- Megmagyarázhatatlan újraindulások,
- Ismert programok szokatlanul viselkednek (szokatlan üzenetek stb.),
- Ismeretlen hálózati kapcsolatok, amelyek soha nem kapcsolódtak a rendszerhez.

Az eltulajdonítás tényét rögtön jelezni kell!

Ahhoz, hogy megfelelően kezelni lehessen egy támadást, nézzük meg, milyen lépésekkel kell úrrá lenni rajta:

1. lépés: **A pánik elkerülése!**

Egy betörés észlelésének alkalmával a legkézenfekvőbb jelenség, hogy stresszes állapotba kerülünk. Ilyen esetben fontos a nyugalom megőrzése. Az idegeskedés okozta stressz olyan dolgokra képes, amelyekkel csak rontani lehet a kialakult helyzeten.

Első lépésként tisztázni kell magunkban néhány kérdést:

- Valóban történt betörés? Azt a jelenséget, amit esetleg a betolakodó jelenlétére utaló jelnek ételmezünk, eredményezheti egy software, vagy a használatból eredő hiba is.
- Valóban történt bármilyen károkozás?
- Fontos, hogy a rendszert minél hamarabb visszaállítsuk normál állapotába? (mert a támadás bizonyításához esetleg szükséges lesznek olyan adatok, melyeket könnyen törölhet egy rendszer visszaállítás)

2. lépés: **Az esemény dokumentálása!**

Talán furcsának hangzik, de sokat segíthet a későbbiekben, ha egy a kezünk ügyébe kerülő papírlapra, feljegyezzük a történéseket időrendi sorrendben. (mi történt, mikor, támadás jellege, stb) Ez elősegíthet abban, hogy megfelelően tudjunk felkészülni egy hasonló támadásra a jövőben.

3. lépés: **Értesítési kötelezettség!**

A támadási esemény észlelésekor a biztonsági felelőst és/vagy a közvetlen főnököt kell értesíteni. Amennyiben megfelelően voltak elvégezve a preventív védelmi eljárások, és a felhasználói oktatás alkalmával elsajátított korábbi támadások ismeretére alapozva létrejött egy elhárítási terv, akkor az ide vonatkozó biztonsági elemeket kell alkalmazni. Az értesítést célszerű független kommunikációs eszköz igénybe vételével elvégezni. Értelemszerűen, ha a kézi számítógépet érte támadás, akkor kerülni kell az azon való beszámolást a történtekről, hiszen a támadó olvashatja a kimenő e-maileket, és egyéb üzeneteket.

4. lépés: **A helyzet elemzése!**

Természetesen, ha a készüléken tárolt információ jellege azt megkívánja, akkor az észleléskor azonnal meg kell szüntetni a hálózati kapcsolatot, vagy egyszerűen ki kell kapcsolni a készüléket. Ez ugyan a behatolótól való megszabadulás legegyszerűbb módja, de azzal jár, hogy félbeszakítja a gépünkön folyó összes munkafolyamatot és esetleg adatvesztést is okoz az el nem mentett adatokban.

A detektív védelmi intézkedésekkel megelőzhetőek azok a nemkívánatos események, amelyek lehetséges következményei akár:

- Az információ megváltozását vagy elvesztését;
- Az információ (beleértve minősített adatokat is) illetéktelen kezekbe kerülését;
- Személyek vagy csoportok jó hírének károsodását;
- Bizalomvesztést, és vagyoni veszteséget okozhat;

Azt mindenképpen szem előtt kell tartani, hogy a legtöbb behatolás egy már kompromittálódott felhasználói jelszó következménye.

3.3 Korrektív védelmi intézkedések

Amint azt megvizsgáltuk, az elhárító kontrollok szerepe az, hogy még időben beavatkozzanak az esetleges rendellenes események folyásába és kiküszöbölje az abból a későbbiek során felmerülő károkat. A korrektív intézkedések célja a hibamentes normális állapot visszaállítása, a nem kívánt esemény bekövetkezése után minél előbb,

valamint a felkészülési tevékenységek (pl. biztonsági mentések, a katasztrófa elhárítási terv) elvégzése.

Amennyiben nem sikerült a megelőzés, majd azt követően az észlelés, és az észlelést nem követte megfelelő időben a reagálás, és így a támadás sikere részlegesen vagy teljesen be is következett, akkor lép színre a fennmaradó fenyegetések ellen az elhárító kontroll.

Ezek az intézkedések részben az észleléshez is köthetők, illetve a korrektív intézkedés eredményezhet a későbbiekben egy megelőző intézkedést. Ki kell hangsúlyozni azt, hogy az elhárító kontrollok a katasztrófa előtti utolsó intézkedések lehetnek, vagyis, ha egy rendszerben nincs beépítve, akkor a megelőzésből és az észlelésből adódó előnyök is csökkenhetnek a rendszer védelmében tett intézkedések tekintetében.

A korrektív intézkedések közé sorolhatóak a következők:

- **Kívánt állapotba hozás**. Ez többnyire valamilyen törléssel, újraindítással vagy előző állapot visszaállításával oldható meg, mint például a vírusirtás, rendszer újraindítása, rosszindulatú alkalmazás leállítása, törlése.

- **Módosítás**. Ide tartozik a jogosultságok változtatása (jelszóváltoztatás, hozzáférési jogok korlátozása).

- **Helyreállítás**. A katasztrófaterv szerinti eljárás követése, hogy a rendszer szolgáltatásai mielőbb rendelkezésre álljanak, de legalább a károk kezelése megtörténjen. A helyreállítás történhet az adott eszközzel (mentésből visszatöltés), vagy tartalékrendszer igénybevételével.

3.4 Biztonsági mentések

A biztonsági mentés célja, hogy biztosítsa az információ és az adatfeldolgozó szoftverek épségét és rendelkezésre állását. Lényege a teljes, veszteségmentes visszaállíthatóság. Minden adatmentésre alkalmazott eszköz (szoftver, vagy hardver) első üzembe helyezése előtt ki kel próbálni az adat-visszaállítást egy másik gépen, vagy egy tesztkönyvtárban. A biztonsági mentéseket megfelelő szintű fizikai és környezeti védelemmel ajánlatos ellátni úgy, hogy a mentési médiák az esetleges rongálódástól meg legyenek kímélve. A mentések típusa (pl. teljes vagy differenciált mentés) és a gyakorisága álljon arányban a mentett adatok minősítésével, fontosságával. A biztonsági mentéskor létrejött adatok legalább három generációját ajánlott visszamenőlegesen megőrizni.

Az üzletmenetet biztosító adatok és szoftverek biztonsági mentésének időszakos elkészítése, valamint ellenőrzése alapvető biztonsági követelmény.

3.4.1 Biztonsági mentések készítése

A folyamatosan biztonsági mentések készítésével, elkerülhető az adatvesztést okozó jelenségek által okozott károk jelentős része. A kézi számítógépek világában a biztonsági mentést a különböző szoftvergyártók termékeivel lehet kényelmesen megoldani, amiket akár komplett csomagokban lehet megvásárolni.

Ezek egyike az SPB Backup és az SPB Clone nevezetű szoftver páros. Az előbbivel biztonsági másolatot készíthetünk a PDA- n található fájlokról, beállításokról. Probléma esetén pedig a program segítségével könnyedén visszaállíthatóak a sérült adatok.

Jelszavas titkosítás mellett végezhetünk vele:

- Teljes biztonsági mentést, ahol az összes rendszeradat, e-mail, dokumentum, PIM adat mentésre kerül.
- Személyre szabott mentést, ahol kiválasztható, hogy az előbbi lehetőségek közül mik azok, amelyeket menteni szeretnénk.
- Időzített mentést, aminek esetében testre szabhatjuk, hogy a program a hét melyik napjain, milyen időpontokban végezze el a biztonsági mentést.

Természetesen az adatok biztonsági mentése, a minden PDA operációs rendszerén elérhető asztali számítógéppel történő szinkronizáló kapcsolattal is megoldható. Ennek alkalmazása - függetlenül az előbb említett szoftveres adatmentéstől - ajánlott, hiszen így fizikailag nem egy adathordozó eszközre kerül a mentett és a mentendő állomány, hanem két egymástól független helyen (a készülék memóriakártyáján és az asztali számítógép merevlemezén) keletkezik mentett adat, ami már eleget tesz a biztonságos tárolás követelményének. Fontos megemlíteni, hogy a biztonsági másolat minden, adatvédelmi szempontból érzékeny adatot tartalmaz, így az archívum tárolásakor ugyanolyan gondossággal kell velük eljárni, mintha „éles” adatok lennének.

Az Spb Clone abban különbözik az Spb Backup-tól, hogy az egész operációs rendszerről képes készíteni egy másolatot, úgynevezett klón állományt, amivel egy Hard Reset után is visszaállítható a teljes rendszer. Ebből a klónból azután egy másik

hasonló típusú (egy, vagy több) készülékre is felmásolható, mintegy tükrözhető az állomány.

Láthatjuk tehát, hogy az elhárító kontroll még helyrehozhatja a támadás következményeit, akkor is, ha a támadás sikeres volt, de jelentősebb károkozás nem történt.

4. Fejezet

Miről szól ez a fejezet?

Ebben a fejezetben meg szeretném vizsgálni azt a kockázatot, amit a vezeték nélküli, nyílt vagy gyenge titkosítást használó hálózat kiépítés rejt magában. A megfelelő védelem hiányában a rendszer biztonsági réseit kihasználva a támadás hozzáférhet a tárolt adathoz, a jelszóhoz, és „belehallgathat” a hálózati forgalomba.

4.1 Támadási forgatókönyv

Vizsgálatom forgatókönyve szerint egy vezetékmentes hálózat felderítését, a jelszavának megszerzését, valamint az útválasztó eszközhöz (router) csatlakozó kézi számítógépe fontos adatait kísérelem megszerezni. A jelszó megszerzése arra is rávilágít, hogy miért olyan fontos a biztonságos jelszó megalkotása.

A támadást a BackTrack3 nevű programcsomag eszközeivel hajtom végre, amely ingyenesen letölthető a készítők honlapjáról. Egy asztali számítógépről hajtom végre a támadást, ami teljesen független a routertől, és az áldozat szerepét betöltő kézi számítógéptől. A vezetékmentes hálózat elérését, lehallgatását és a csomagok elfogását egy beépített hálózati kártya segíti.

Mint az a (2.2.2.2) „A vezetékmentes hálózatok fenyegetései” - című fejezetrészből kiderül, a WEP titkosítás már elavult, könnyedén feltörhető, ezért én a manapság legbiztonságosabbnak tartott titkosítás kulcsának megszerzésére törekszem. A védelemhez egy 13 karakterből álló jelszót választottam, ami tartalmaz kis és nagybetűt, valamint számot.

A jelszó a következő: GyengeJelszo1 **A titkosítás:** WP2-PSK

A támadás a következő lépések sorrendjében történik:

- A hálózat felderítése és a célpont azonosítása.
- Az útválasztó és a célpont közötti csomagok megszerzése.
- Az elfogott adatcsomagokból szótáras módszerrel kinyerjük a kulcsot.

A támadás megkezdésekor feltételezzük, hogy a támadónak semmilyen információ nem áll rendelkezésére a hálózat kiépítéséről, jelszaváról, így mintegy „vakon” végzi a támadást.

4.1.1 A hálózat felderítésére szolgáló eszközök bemutatása

Azokat a szoftver és hardver eszközöket tekinthetjük meg az 6. táblázatban, amelyek a vizsgálat elvégzéséhez szükségesek.

Eszköz neve		Leírása
BackTrack3 (Linux)		A legújabb biztonsági szoftver csomag, amit egyaránt használnak előszeretettel a támadásokhoz éppúgy, mint biztonsági szakemberek a hibák felderítéséhez. Egyszerű, telepítést nem igényel, hiszen az elemzési platform közvetlenül egy cd lemezről indítható el és perceken belül teljesen hozzáférhető (ú.n LiveCD, vagyis telepítés nélkül boot[42]-olni képes). Jelenleg BackTrack 300-nál több olyan különböző, naprakész eszközt tartalmaz, amiket a biztonsági szakértők munkafolyamata szerint strukturáltak. Ezen kívül még számos program áll rendelkezésre egy támadás kivitelezéséhez, azonban hosszabb előzetes vizsgálat után ennek a programcsomagnak a használatát tartom a feladat elvégzésére alkalmasnak. Beszerzési forrás: http://www.remote-exploit.org/backtrack_download.html
Airodump	**BackTrack3 csomag részei**	A WiFi hálózat felderítésére és lehallgatására alkalmas program.
Aireplay		A feladata a csomagok elfogása és hálózatba való visszaküldése. Ezzel az eszközzel fogjuk el az áldozat és a hozzá kapcsolódó router közötti forgalmat, az ARP[43] csomagokat, melyekből kinyerhető a kulcs.
Aircrack		A kulcs feltörésére alkalmas szoftver.
Szótár		A jelszó megfejtéséhez a http://www.passwords.ru/ és az ftp://ftp.ox.ac.uk/pub/wordlists/hungarian/ weboldalakról beszerezhető szótárfájlokat használtam.
Útválasztó eszköz		Linksys WRT54G Wireless-G Broadband Router
Hálózati kártya		D-Link AirPlus Xtreme G DWL-G520 Adapter

[42] A számítástechnikában a boot egy több részből álló folyamat, melynek során az operációs rendszer beindul.

[43] MAC address és IP – címeket tartalmazó adatcsomag.

Kézi számítógép (áldozat)	ASUS MYPAL PocketPC A696 (Wondows Mobile 6.0 magyar nyelvű operációs rendszer)
Asztali számítógép (támadó)	Intel(R) Core(TM)2 Duo CPU E8200@2.66GHz, 2 mag
Internet	Ez az eszköz talán a legfontosabb mind közül, hiszen innen szerezhető be a támadás elvégzéséhez a **legtöbb**, **bárki** számára elérhető információ.

6. táblázat A vizsgálat során alkalmazott eszközök.

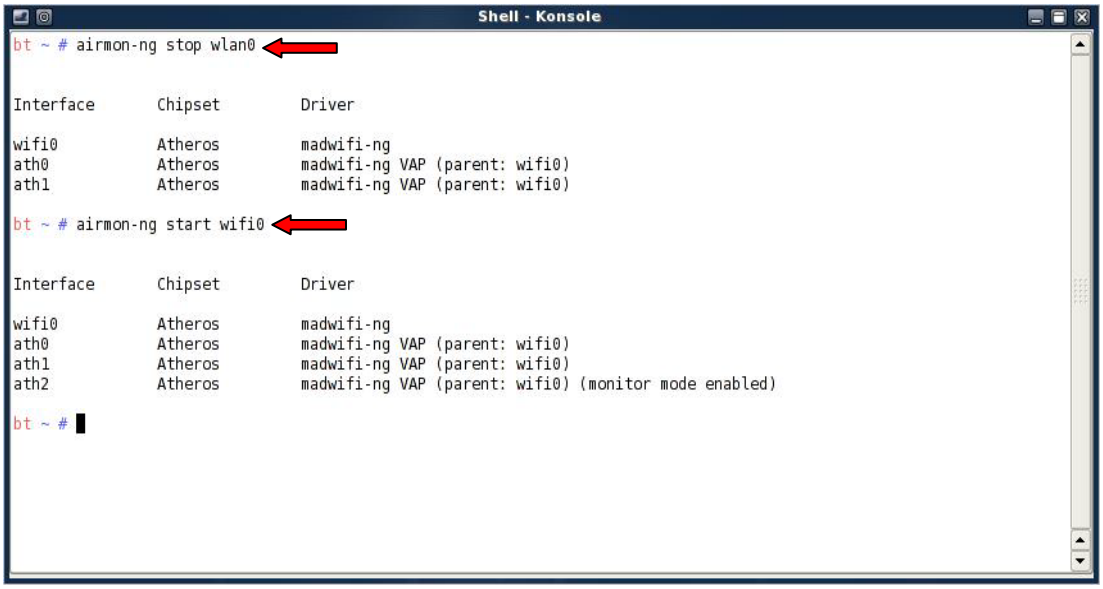
4.1.2 Betörés a vezeték nélküli hálózatba

A támadás megkezdése előtt üzembe helyezzük a támadó és az áldozat szerepét betöltő készülékeket, valamint létrehozzuk a router és a kézi számítógép közötti vezetékmentes kapcsolatot. A LiveCd-t behelyezzük az asztali számítógép CD-ROM meghajtójába és végigvárjuk a boot folyamatot. A bejelentkezést követően a tálcáról elérhető Shell-konzolt megnyitjuk. Ezen keresztül fogjuk a parancsokat begépelni, és itt kísérjük figyelemmel a program folyását, valamint a konzol segítségével ellenőrizzük majd a támadás kimenetelét. A használt parancsoknak van egy általános szintaktikája, amit az alábbi táblázatban tekinthetünk meg:

A parancsok általános felépítése
A sorrendiség megtartásával: [program meghívása] < alprogram meghívása > (feladat) / eszköz /
Például: [airmon-ng] <nincs alprogram> (stop) / wlan0 /

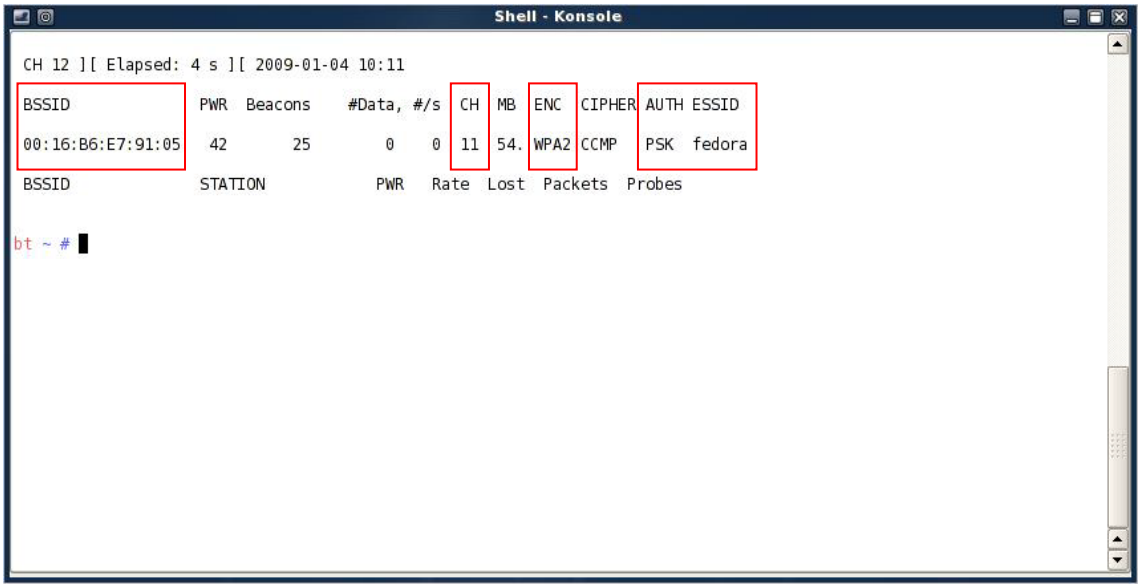
7. táblázat Shell parancs felépítése.

Az első parancs azért szükséges, hogy megállítsuk a hálózati adapter vezetékes működési módját. Ehhez az **airmon-ng stop wlan0** parancssort gépeljük be, majd a következő lépésben az **airmon-ng start wifi0** parancssorral bekapcsoljuk a vezetékmentes módot, a vizsgálat megkezdéséhez. Az utasításokat piros nyíllal emelve ki a kimenetét az alábbi ábrán láthatjuk:



9. ábra A hálózati adapter üzemmódjainak ki/be kapcsolása.

Amennyiben nem kaptunk hibaüzenetet akkor a hálózati kártya készen áll. Ezután az **airodump-ng ath1** parancs meghívása következik, mellyel a WiFi hálózatot tudjuk megkeresni, majd adatokat rögzíteni vele egy fájlban. A parancs elvégzése után a következő, számunkra fontos adatokhoz jutunk:



10. ábra Az airodump által talált hálózati kapcsolat.

A piros kerettel kiemelt adatok leírását megtaláljuk a 8. táblázatban.

Név	Leírás
BSSID	Az útválasztó MAC address-e. (00:16:B6:E7:91:05)
CH	A csatorna, amelyiken a kommunikáció folyik. (jelen esetben a 11-es)
ENC	A titkosítás. (WPA2)
AUTH	A titkosítás kulcsának típusa. (PSK - előre megosztott kulcs)
ESSID	A vezetékmentes hálózat elnevezése. (a routerben beállított)

8. táblázat Az airodump által megjelenített adatok.

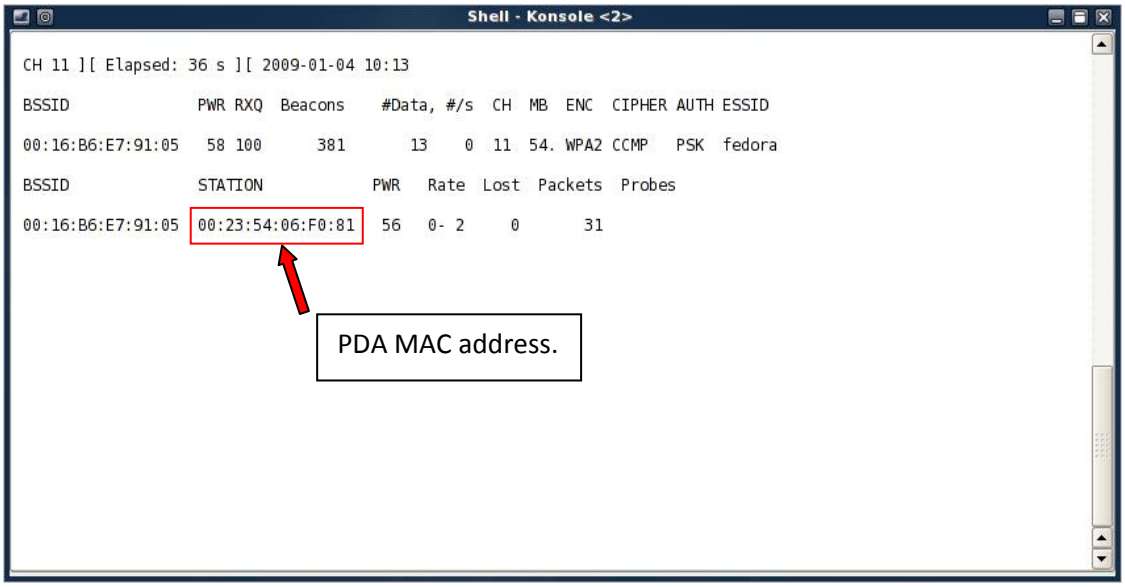
Az így megszerzett adatok birtokában elvégezzük az **airodump-ng -c 11 -w adatok --bssid 00:16:B6:E7:91:05 ath1** begépelésével a fontos információk fájlba mentését.

Nézzük meg részletesebben ezt a parancsot:

Parancs	Feladata
airodump-ng	Meghívja a programot ami lementi a csomagokat, amiket majd az **aircrack** program tud felhasználni a jelszó megszerzéséhez.
-c 11	Kiválasszuk a csatornát, ahol a kommunikáció folyik.
-w adatok	Létrehozzuk az „adatok” nevű fájlt **.cap** és **.txt** kiterjesztéssel (egy alapértelmezett mappába kerül).
--bssid 00:16:B6:E7:91:05	A router MAC addresse. A rajta keresztül kapcsolatban lévő eszközök megkeresése.
ath1	A támadó gép hálózati kártyájának elérése.

9. táblázat A kibővített airodump parancs.

A parancssor lefutásának eredménye a 11. ábrán látható. Itt már megjelenik a hálózathoz csatlakoztatott kézi számítógép MAC address-e is a STATION oszlopban.



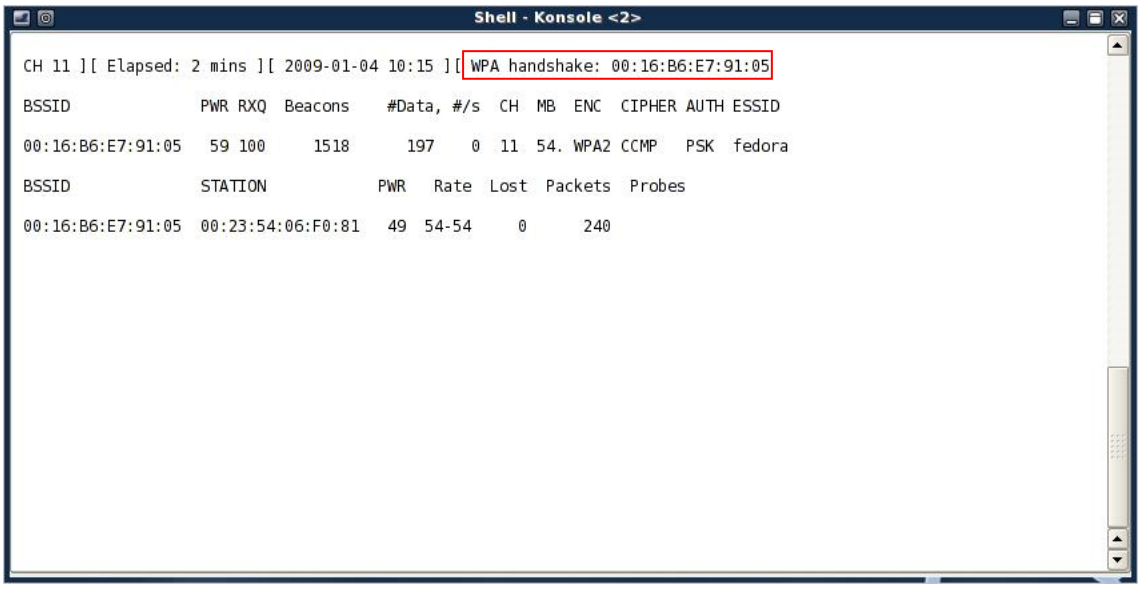
11. ábra Megjelentek a kapcsolódó PDA adatai.

Idáig eljutva is már értékes információkhoz jutottunk. Ezután az **aireplay-ng -0 1 -a 00:16:B6:E7:91:05 -c 00:23:54:06:F0:81 ath1** parancs segítségével elfogjuk a jelszó megszerzéséhez elengedhetetlen csomagokat. A program az alábbi feladatokat hajtja végre nekünk:

Parancs	Feladata
aireplay-ng	Csomag elfogása a hálózatból.
-0 1	A hozzáférés elindításának alprogramja.
-a 00:16:B6:E7:91:05	A router (MAC address szerint azonosítva)…
-c 00:23:54:06:F0:81	és az áldozat PDA (MAC address szerint azonosítva) adatforgalma közötti csomagok megszerzése.
ath1	A támadó gép hálózati kártyájának elérése.

10. táblázat A hálózati csomagok megszerzéséhez szükséges parancs.

Az aireplay program használatával a router és a PDA közötti csomagok elfogását végeztük el. A kimenetet és a sikeres végrehajtást a 12. ábrán láthatjuk.



12. ábra Az aireplay parancs lefutása után megjelenő kapcsolat.

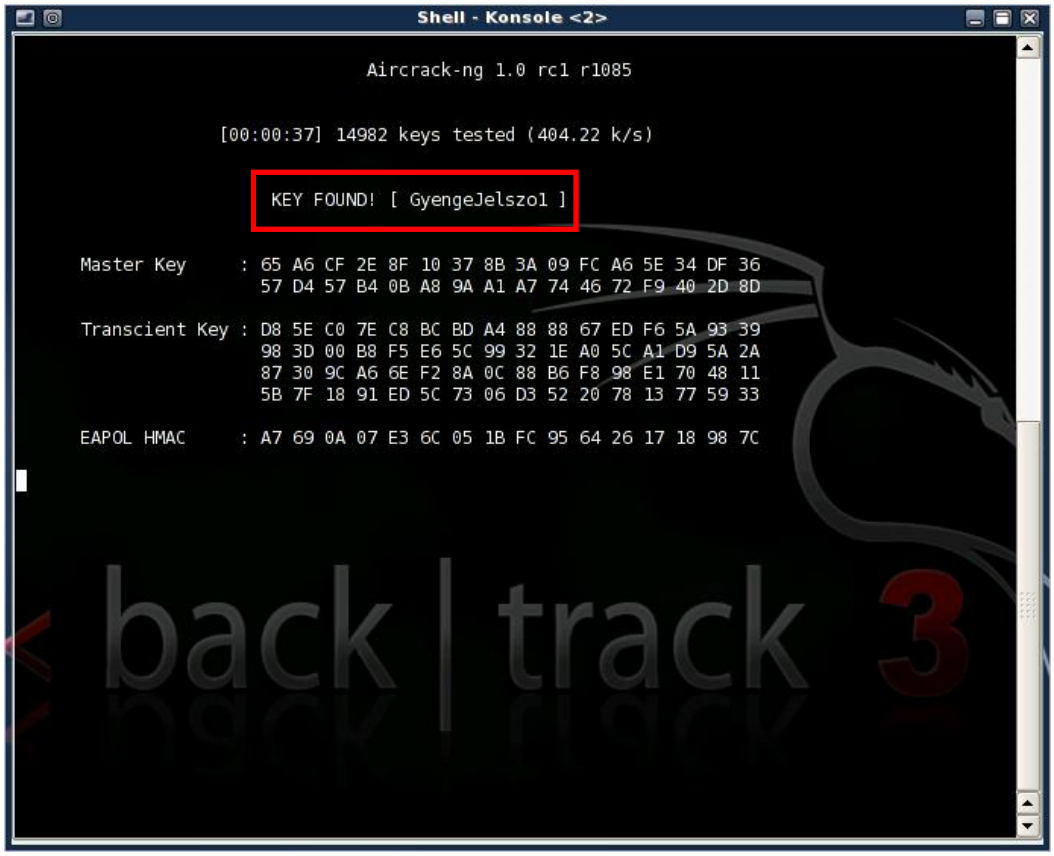
A jelszó megszerzéséhez már csak egyetlen parancsot kell megadni, az **aircrack-ng -w allwords.txt -b 00:16:B6:E7:91:05 adatok*.cap** sor begépelésével. Ekkor elindul egy keresési folyamat, melynek során az allwords.txt nevű fájlból (ami egy password dictionary) a program azonosságokat keres.

Parancs	Feladata
aircrack-ng	A jelszó megszerzését végzi.
-w allwords.txt	Az itt megadott fájlból keresi ki az egyezéseket….
-b 00:16:B6:E7:91:05	a router (MAC address szerint azonosítva) és az áldozat PDA közötti adatforgalomból eltárolt csomagjait őrző fájl segítségével.
adatok*.cap	

11. táblázat Az aircrack program szükséges parancsai a jelszó töréséhez.

A helyes jelszó megválasztása sorsdöntő, mert a rosszul megválasztott jelszó segítségével a támadó hozzáfér a hálózathoz, és azon keresztül a rá kapcsolódó kézi számítógéphez és egyéb eszközökhöz.

A keresés végeredményét a 13. ábra ismerteti:



13. ábra A jelszó megfejtése.

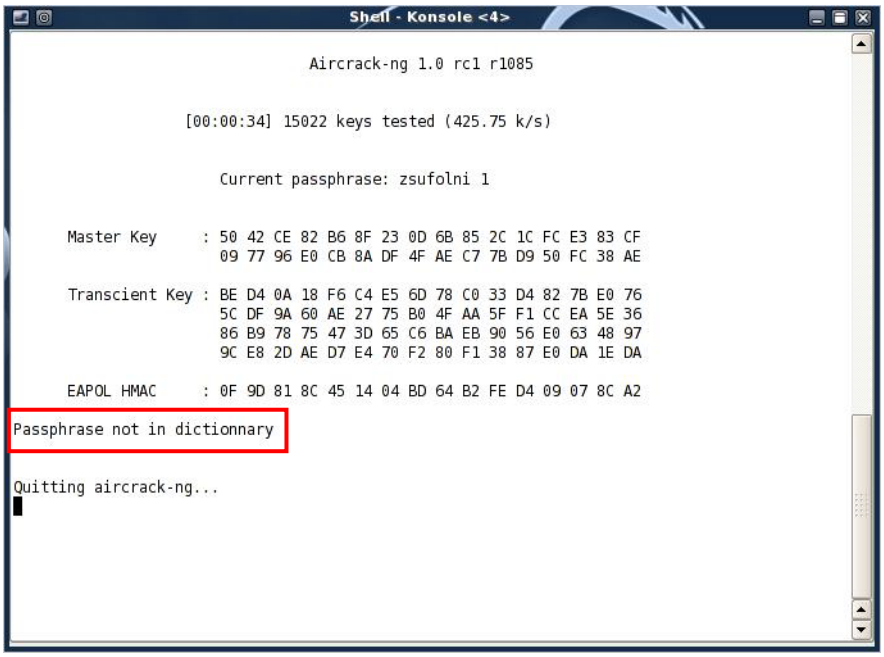
Mint láthatjuk, hiába adtunk meg megfelelő hosszúságú, kis és nagybetűt, valamint számot tartalmazó jelszót. Amennyiben az belefér a szótári szavak kategóriájába, akkor szótáras töréssel kinyerhető a csomagokban megbúvó hozzáférést biztosító jelszó.

A támadásnak van még egy **veszélye**, hiszen megmutatja az áldozat PDA MAC addressét. Ennek birtokában a MAC szűrést alkalmazó hálózatba már bármikor képes bejutni a támadó, hiszen a hálózat résztvevői felé hamis MAC cím küldésével és a feltört jelszó megadásával „jogosulttá” válik annak használatára.

Természetesen megvizsgáltam azt is, hogy mi történik akkor, ha olyan jelszót használunk a kommunikáció titkosítására, ami megfelel a biztonságos jelszó kritériumának. Ehhez előbb módosítottam a jelszót az útválasztó Wireless Security elnevezésű paneljén a következőképpen:

14. ábra A biztonságos jelszó beállítása a routeren.

Az új jelszót a már megismert „A kézi számítógépek biztonsága elsődleges és lényeges.” - mondatból képeztem. Az előzőekben bemutatott eljárásokat újfent elvégezve a 15. ábrán látható eredményt értékelhetem ki:



15. ábra A biztonságos jelszót nem tudja megfejteni.

Mire következtethetünk ebből?

Arra, hogy a kulcs megszerzésére csak akkor válik lehetőség, amikor értelmes szavakból, szótári szavakból állítottuk össze, és nem vettük figyelembe, hogy a WPA2-PSK titkosítás törése a gyengén megválasztott jelszavak esetében ugyanúgy sikerülhet, mint az elavult és ezért háttérbe szorult WEP titkosításnál.

4.2 Biztonsági ajánlások

Az előző fejezetek során megismerkedtünk a kézi számítógépek törtnetével, fejlődési irányaival, valamint az őket fenyegető veszélyforrásokkal és a sebezhetőségeikből adódó biztonsági gyengeségeikkel. Megvizsgáltuk, milyen támadásoknak vannak kitéve ezek az eszközök és a védekezési intézkedések hogyan, milyen módon tudják befolyásolni a támadások kimenetelét.

Itt most néhány olyan ajánlás kerül felsorolásra, amelyeknek a betartásával csökkenthető a kézi számítógépek biztonsági kockázata.

Az ajánlásokat három kategóriára bonthatjuk fel:

Technológiai, Használati, Szabályzati.

Technológiai ajánlások:

Ide soroljuk azokat a tanácsokat, melyek a készülék biztonságos munkavégzésének a feltételei.

- Az eszköz alapértelmezett beállításainak megváltoztatása!
- A készüléken használt szoftvereinek ellenőrzött telepítései és beállításai.
- Megfelelően erős jelszavas védelem kialakítása, mind a készülék, mind a hálózat használatának vonatkozásában!
- Az ellenőrzött frissítések szakszerű telepítése!

Működtetéssel kapcsolatos ajánlások:

A mindennapi használattal, és a kommunikációval foglalkozó ajánlások.

- Soha ne csatlakozzunk Ismeretlen hálózatokhoz!
- Amennyiben nincs rá feltétlenül szükség, a Bluetooth kapcsolatot inaktívvá kell tenni.
- A vezetékmentes kapcsolat kiépítését, csak megfelelő titkosítás után engedélyezzük!

- Használjunk biztonsági szoftvereket! (vírusirtót, felhasználói jogosultságot kezelő, biztonsági mentést segítő szoftverek)
- Rendszeresen frissítés ellenőrzés!
- Az eszközhöz való hozzáférést megfelelő jelszavas védelemmel kell szabályozni. (Eltulajdonítás)
- Ahol csak lehetséges és az adat titkosítás ezt megköveteli, alkalmazzunk felhasználó hitelesítést! (tudás-, birtok-, biometria alapú azonosítás)
- A cég központjával folytatott vezetékmentes kommunikáció során használjunk olyan titkosítási es hitelesítési megoldásokat, melyek biztosítják az adatok sértetlenségét, bizalmasságát és rendelkezésre állását! (megoldást jelenthet a VPN használata)

Szabályzati ajánlások:

A kategória olyan intézkedéseket foglal magában, amelyek irányelvet nyújthatnak egy cég által használt kézi számítógép eszközállomány biztonságos kezeléséhez.

• A felhasználók megfelelő szintű képzése a vezeték nélküli hálózatok és a készülékek biztonságos használatára, valamit az elsajátított tudás szinten tartásának biztosítása, számonkérése!

• Biztonsági szabályzat létrehozása, vagy kiterjesztése a kézi számítógépek használatára!

• Kockázatelemzés a fenyegetettség mértékének megismerésére! (Rendszeres időközönkénti felülvizsgálattal.)

• A felhasználóknak a használatra vonatkozó jogainak és kötelezettségeinek a meghatározása!

• Pontos dokumentáció vezetése a meglévő kézi számítógépekről. (biztonsági frissítések, felhasználók adatai, karbantartások, stb…)

Összefoglalás

Amint azt láthattuk, a nem megfelelően védett kézi számítógép használata egyre veszélyesebb. Életünk, munkánk során segítségre lehetnek, de kárt is okozhat a felületes használatuk. Ezeknek az eszközöknek az előnyeit akkor tudjuk igazán kihasználni, ha náluk is képesek vagyunk megvalósítani az asztali számítógépeknél szokásos biztonsági szintet. Ez persze nem könnyű feladat, de betartva néhányat az ajánlott lépésekből, melyek növelik e készülékek biztonságát, számottevően megnehezíthető egy támadás sikeressége. Az előző fejezetekben utána jártunk annak, hogy képesek lehetünk-e megvédeni a készüléket és a rajta tárolt információt. Megvizsgáltuk a legjellemzőbb sebezhetőségeit, a leggyakoribb fenyegetéseket, és az ellenük alkalmazható védekezési lehetőségeket.

Bizonyára felvetődik a kérdés, hogy meddig lehet fokozni, el lehet-e érni a tökéletes biztonságot? A válasz egyértelműen nem! A biztonság egy olyan állapot, melyben a kockázat minimalizálásával párhuzamosan csökkentjük a fenyegetést. A teljes biztonság állapota bizonyos rendszerek - mit például a felhasználó - kizárását kellene, hogy eredményezze, akkor pedig a működésének lényegét veszítené el a készülék. A gyártóknak és a fejlesztőknek törekedniük kell a biztonságos megoldások folyamatos fejlesztésével a felhasználók alapvető hibáinak a kiszűrésére csakúgy, mint az egyéb támadások hatékony elhárítására.

Addig azonban, amíg mi felhasználók nem tartjuk magunkat egy - akár saját magunk által elfogadott - biztonsági szabályrendszerhez, amíg nem változik a hozzáállásunk a kézi számítógépünk biztonságos működtetésével kapcsolatban, addig mindig célpontjaivá válhatunk a támadásoknak.

Elérte a dolgozat a célját? Megváltozott az olvasónak a hozzáállása a kézi számítógépének biztonságban betöltött szerepéhez? Amennyiben legalább egy gondolat erejéig foglalkozott a biztonságos használattal, akkor mindenképpen, hiszen elindult azon úton, melyen minden egyes lépéssel közelebb kerül a **kielégítő biztonsághoz**.

Irodalom jegyzék

Könyv:

1) Jeff Crume, **Az internetes biztonság belülről…amit a hekkerek titkolnak**, 2003, Bicske, Szak Kiadó.

2) Bodlaki Ákos, Csikely Judit, Endrédi Gábor, Farmosi István, Dr. Haig Zsolt, Hajnal János, Jakab Péter, Dr. Komor Levente, Dr. Kovács László, Kovács Tamás, Dr. Kőrös Zsolt, Mosolygó Ferenc, Muha Lajos, Nagy Béla, dr. Nagy Gábor, Dr. Nagyné Szilvási Mária, Dr. Nemetz Tibor, Nyitrai Miklós Zoltán, Dr. Nyíry Géza, Sajti János, Dr. Szenes Katalin, Szigeti Szabolcs, Unicsovics György, Vadász Dezső, Dr. Váncsa Julianna, Dr. Ványa László, Dr. Verebics János, **Informatikai biztonság kézikönyve**, 2008, Budapest, Verlag Dashöfer Szakkiadó Kft.

3) David Kammer, Gordon McNutt, Brian Senese, Jennifer Bray, **Bluetooth Application Developer's Guide: The Short Range Interconnect Solution**, 2002, USA, Syngress Publishing.

4) Danny Briere, Pat Hurley, **Wireless Network Hacks & Mods For Dummies**, 2005, Indianapolis, Wiley Publishing.

Előadás vázlatok:

5) http://www.tilb.sze.hu/tilb/targyak/NGB_TA0028_1/Halozatok_biztonsaga_0.311.pdf , Hálózatok biztonsága , 2008-12-24

6) http://www.krasznay.hu/presentation/ethical_hacking_krasznay.ppt , Ethical Hacking, 2008.10.10

Internet:

7) http://www.cert.hu/dmdocuments/MTA1_print.pdf , Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai, 2008-12-23

8) http://www.pdamania.hu/content/2105 , PDA Mánia cikkek, 2008.10.03

9) http://www.ekk.gov.hu/hu/kib/ajanlasok , Közigazgatási Informatikai Bizottság ajánlásai, 2008.10.03

10) http://enc.phil-inst.hu/enc.htm , Magyar Virtuális Enciklopédia, 2008.10.03

11) http://ipod-touch.ath.cx/index.php?option=com_content&task=view&id=88&Itemid=2 , 2008.10.06

12) http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/elohazi_rw7.html , Mobil eszközök biztonsági problémái, 2008.09.30

13) http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/munk_rw7.html , Információbiztonság vs. Informatikai biztonság, 2008.09.30

14) http://vil.nai.com/vil/content/v_145451.htm, Trójai jelentés, 2008.11.09

15) http://www.symbian.com/symbianos/index.html , A Symbian rendszer hivatalos honlapja, 2008.10.06

16) http://www.krasznay.hu/presentation/diploma_spala.pdf , Diplomamunka Spala Ferenc, 2009-01-02

17) http://itszotar.hu/ , Informatikai szótár, 2008.10.10

18) http://www.nokiaprogramok.hu/modules.php?name=News&file=print&sid=457 , 2008.10.12

19) http://www.arionet.hu/ ,2008.10.13

20) http://www.computerworld.hu/trojai-program-pda-ra.html, 2008.10.19

21) http://www.tricon.hu/~mcree/ellpaszt/ellpaszt_7.5.pdf, 2008.10.15

22) http://www.biztostu.hu/ , 2008.11.11

23) http://www.macnewsworld.com/story/35645.html, 2008.11

24) http://ftp.icm.edu.pl/pub/unix/security/wordlists/ 2008-12-12

25) http://www.filewatcher.com/b/ftp/ftp.mayn.de/pub/really_old_stuff/unix/security/wordlists.0.0.html , 2008-12-12

26) http://www.windowsceportal.hu/index.php?tartalom=oprendszerek&id=c5203p PPC 6 adatlapja, 2008-12-27

27) http://www.windowsceportal.hu/index.php?tartalom=oprendszerek&id=c5213p PPC 6.1 adatlapja, 2008-12-27

28) http://www.gore.com/en_xx/products/electronic/specialty/antitamper.html , 2008-12-24

29) http://www.google.hu/search?hl=hu&client=firefox-a&rls=org.mozilla%3Ahu%3Aofficial&hs=kkI&q=allintext%3A+pda+security&btnG=Keres%C3%A9s&meta= , 2008-12-24

30) http://www.cert.hu/index.php?option=com_content&task=blogcategory&id=64&Itemid=66 , 2008-12-28

31) http://matyascsaba.extra.hu/index.php?option=com_content&task=view&id=320&Itemid=122 , 2008-12-30

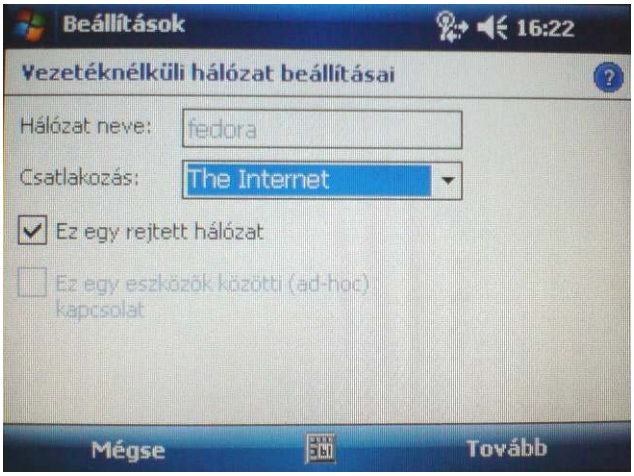
32) http://www.it-business.hu/index.php/technologia/21355-zsebre-vagott-iroda?searchword=windows+mobile , 2009-01-01

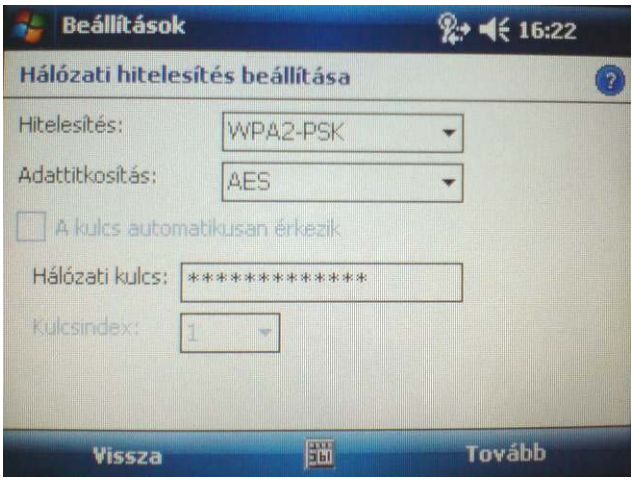
33) http://www.bpcomp.hu/adatvedelem.php?safesoft=sg_pda, SafeGuard, 2008-12-06

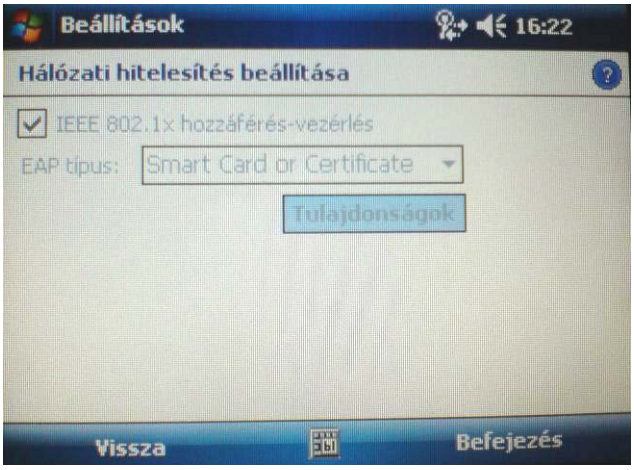
Mellékletek

1. Számú melléklet.

A PDA vezetékmentes kapcsolatának beállítási lépései:







2. Számú melléklet

A Bluetooth beállításának lépései.