Információbiztonság, technikai alapismeretek

Dr. Keszthelyi András

Óbudai Egyetem, Keleti Károly Gazdasági Kar

Szervezési és Vezetési Intézet

keszthelyi.andras@kgk.uni-obuda.hu

Absztrakt: Jelen írás két nagy területet érint: adataink maradjanak meg használható formában számunkra, ezen túl pedig illetéktelenek ne férjenek hozzájuk. A legelemibb alapfogalmak (adat, információ, ismeretszerzési folyamat), és a valós meg a virtuális világ néhány jellegzetes különbségének áttekintése után számba veszi a fontosabb veszélyeztető tényezőket, az esetleges motivációkat, majd áttekinti, mi mindent tehetünk, illetve kell tennünk adataink megmaradása és az illetéktelenek kizárása céljából. Ezen belül tárgyalja a biztonsági mentések főbb szempontjait,a védelem három síkját (fizikai, ügyviteli, algoritmusos), ezen belül kiemelten a jelszavak alkalmazásának korlátait és problémáit. Az illetéktelen hozzáférés elleni védelem területén az egykulcsos és a kétkulcsos titkosítás elvi alapjait mutatja be, és ismerteti ezek alapvető biztonsági szabályait. A digitális aláírás és a biztonságos böngészés alapjául szolgáló tanúsítványok tárgyalása a kétkulcsos titkosítás olyan gyakorlati példái, amelyeket napi rendszerességgel használunk -- ha nem is minden esetben tudatosan. A terjedelmi korlátok miatt a téma földolgozása felhasználói szempontú és vázlatos. Végül, de nem utolsósorban érinti a magánszféra védelmének néhány vonatkozását, és megemlíti az egész témakör technikai, üzleti, jogi és etikai vonatkozásait.

1 Bevezetés és célkitűzések

A számítástechnika és az informatika mára kiszolgáló (segéd) tudományból alapvető fontosságú szakterületté vált, átszövi mindennapjainkat (vö. „információs társadalom”). Nemcsak a digitálisan tárolt és kezelt adatok mennyisége növekszik napról-napra, de a tőlük való függőségünk mértéke is. Nem kell bizonygatni, hogy ilyen korban jelentősen felértékelődik az adatok védelmének területe, aminthogy felértékelődött az azok megszerzésének eszköztára is.

Gondoljunk csak bele hallgatóként (és a tanulmányi osztály helyében is): mi lenne, ha a tárgyfelvételi időszakban, vagy a záróvizsga előtt két héttel nem működne a Neptun?

Az IEEE biztonságtechnikai és adatvédelmi szimpóziumán 2010 májusában amerikai kutatók olyan problémákra hívták fel a figyelmet, mint például hogy illetéktelenek átvehetik az irányítást már a kocsink[1] fölött is.

Az okostelefonok tulajdonképpen teljes értékű számítógépek, ennek megfelelően számos előnnyel és számtalan veszélyforrással. Az asztali számítógépek védelméről az emberek többsége hallott már valamit, ha esetleg nem is jeleskedik benne, az okostelefonok vonatkozásában azonban a helyzet sokkal rosszabb. Egy felmérés[2] szerint csak androidos okostelefonokra mintegy ötezer kártékony program vált ismeretessé eddig. Márpedig a mobiltelefonba bejutó kártékony program sokkal több kellemetlenséget okozhat általános esetben, mint amelyek asztali számítógépre jutnak be, nem utolsósorban azért, mert a felhasználók sokkal kevésbé vannak tudatában a veszélyeknek.

A kiberháborúk kora elérkezett, már nem lehetőségről beszélünk, hanem arról, hogy ez az állapot (folyamat) a laikus, de gondolkodó emberek számára is jól láthatóan bekövetkezett. Gondoljunk csak a WikiLeaks kiszivárogtatási botrányaira, a Sutxnet vírusra, amely Irán atomprogramjában látványos károkat okozott, vagy az Anonymous „hekktivisták" egynémely akciójára (FBI telefonhívásokat is lehallgattak), stratégiai fontosságú iparvállalatoktól és kutatóintézetektől is lopnak bizalmas és titkos adatokat, esetenként szervezettnek tűnő módon. Az amerikai és angol (kanadai, ausztrál és új-zélandi) állami szakszolgálatok a teljesség igényével próbálják lehallgatni az egész világ elektronikus adatcseréjét, sőt elemezni és értékelni is azt.

Lehetne folytatni a sort...

Ilyen helyzetben talán nem túlzás azt állítani, hogy kiemelt jelentősége van a biztonságtudatos magatartásnak, legyen szó az egyénről mint magánemberről, az egyénről mint valamely cég alkalmazottjáról, vagy magáról a vállalatról. Egy rossz döntés, egy hibás művelet, vagy akár egy gondatlan mulasztás akár katasztrofális következményekkel járhat. Ha valaki ennek kapcsán azt állítaná, hogy nem lehet túlhangsúlyozni a biztonsággal kapcsolatos tudás – elméleti és gyakorlati tudás! – jelentőségét és fontosságát, annak alighanem igaza lenne.

A jelen jegyzet keretei nem elégségesek ahhoz, hogy teljes körű és naprakész tudással vértezzünk fel bárkit is. A technikai háttér- vagy alapismeretekre összpontosítunk, nem tárgyalunk fejlesztői vonatkozásokat (sql-befecskendezés pl.), és amit igen, az sem a teljesség igényével. Ennélfogva biztatunk mindenkit a folyamatos, kitartó önképzésre, tanulásra. Két nagy területet érintünk: adataink maradjanak meg, illetéktelenek pedig ne férjenek hozzájuk.

---

1 Koscher, Karl et al., 2010.
2 Trend Micro Inc., 2012.

2 Alapfogalmak

2.1 Adat és információ

Az adat és az információ fogalma még ma sem egységes és nem is teljesen világos, problémamentes. Mint ahogy a munka és az energia fogalmának letisztulásához, összefüggéseinek világossá válásához is időre volt szükség (nem is kevésre), úgy az adat és az információ fogalmának maradéktalan tisztázásához sem jutottunk még el. Vegyük azonban figyelembe, hogy viszonylag fiatal szakterületről van szó. A tudományos fogalom fejlődése az 1950-es évektől kapott nagy lendületet, a számítógépek fejlődésével és az ún. információs társadalommá vezető fejlődéssel. Jobb és teljesebb megközelítés híján az alábbi gondolatmenetet vesszük alapul.

Különféle értelmező szótárak szerint:

„**adat** fn **1.** Vkinek, vminek a megismeréséhez, jellemzéséhez hozzásegítő (nyilvántartott) tény, részlet. *Gyártási, személyi ~ok.*"

„**data** *lat* ismert tények, adatok, dolgok"

„**data 1.** Factual information, especially information organized for analysis or used to reason or make decisions. **2.** *Computer Science* Numerical or other information represented in a form suitable for processing by computer. **3.** Values derived from scientific experiments." (*számítástudomány* számítógépes feldolgozásra megfelelő formát képviselő számszerű v. más információ).

„**információ** fn **2.** *sajtó* Értesülés, adat. **3.** *Tud* A kibernetikában: berendezésbe jelként betáplált adat; hír. [nk:lat] **~elmélet** fn *Tud* A kibernetikának az információk tárolásával és továbbításával foglalkozó ága."

Az adat magyar nyelvű általános, köznyelvi meghatározása ez esetben közel tökéletes szakmai szempontból is, ellentétben az amerikai angol változattal. Amit nem hangsúlyoz, ami nem nyilvánvaló, hogy a „valaminek" a megismerése nem az *adat* puszta begyűjtését jelenti, hanem a kapott adat a megismerés *lehetőségét* biztosítja. Ami még szükséges, az a kapott adat *értelmezése*. Ahhoz, hogy valami új felismerésre juthassunk újonnan megszerzett adatokból, azt értelmezni kell, meg kell ismerni, vagy fel kell ismerni annak *jelentését* az adott helyzetben. Mondhatjuk tehát, ezt a jelentéstartalmi elemet hangsúlyozva, hogy **az adat értelmezhető, de (még) nem értelmezett ismeret.**

Az értelmezés nem más, mint a kapott új közlés által kiváltott gondolatsor, amely régebben megszerzett tudásunkon, tapasztalatainkon alapul. Ezekkel összevetve az új közlést, következtetést tudunk levonni, és az így megszerzett új ismeret - **a kapott adatnak az adott helyzetben általunk tulajdonított jelentés - az információ.**

Ezen megközelítés egyik következménye, hogy az információ meglehetősen

szubjektív dolog. Ugyanazon adatból különböző helyzetben lévő különböző emberek más-más következtetést vonhatnak le, más-más jelentést tulajdoníthatnak az adott adatnak. Esetleg lehet olyan ember, aki semmilyen jelentést nem tulajdonít neki - akár a szükséges háttérismeretek, akár érdektelensége okán. Ez esetben nem biztos, hogy az adott közlés adatnak tekinthető. Biztosan nem tekinthet adatnak az alábbi párbeszédben felbukkanó, „adatnak látszó közlés”:

A kapitány leordít a gépházba:
- Mennyi?
- Harminc.
- Mi harminc?
- Mi mennyi?

Az információ lényege nem a mennyiség, hanem a minőség – értünk egyet Halassy Bélával. „Az információ minősége összetett jellemző, amelyet különböző paraméterek együtteseként fejezhetünk ki. Ezek többsége nem számszerűsíthető (...) sokszor nehezen definiálható, viszonylagos, a minősítőtől erősen függő sajátosságról van szó.” (Raffai Mária). Az adatbázisok egyik lehetséges felhasználási módja, a szelektív kezelés pont evvel van összefüggésben: olyan új ismeretek megszerzését segítheti elő, amelyeket más, hagyományos eszközökkel csak aránytalanul nehezen vagy egyáltalán nem lehetne megszerezni.

2.2 Ismeretszerzési folyamat

Nem kerülhetjük meg az ismeretek megszerzésének folyamatát, illetve ezen folyamat vizsgálatát. Halassy dr. szerint az ismeretszerzési folyamatnak négy lépése van, az észlelés, az érzékelés, a felfogás és a megértés.

Az **észlelés** az ismerethordozó közeggel való időszerű szembesülés. Az ismeretet mindig valamilyen közeg hordozza. Ha evvel nem találkozunk, vagy nem találkozunk vele időben, nem történhet semmiféle ismeretszerzés. Mivel az ismeret tükrözi a valóság tényeit, az ismerethiány majdnem olyan, mintha az általa tükrözött dolog sem állna rendelkezésre.

Az **érzékelés** lehet a köznapi értelemben vett érzékszervi érzékelés vagy valamilyen eszköz, berendezés által végzett fizikai, műszaki értelemben vett jelérzékelés. Pl. az ép szemű ember képes látni (valamilyen határok között), a számítógépben lévő hálózati (ethernet) kártya képes lehet a hozzá csatlakozó CAT-5-ös kábelen érkező elektromos jelek érzékelésére, kivéve például, ha a muzeális 10 Mbit/s sebességű kártyát próbálnánk meg 1 Gbit/s hálózaton használni.

A harmadik lépcsőfok a **felfogás**. Nem elegendő látni pl. egy „rajzot”, ismerni kell azt a jelkészletet, amelynek az adott „rajz” az egyik eleme. Például, ha az ismeretközlés papírra nyomtatott szöveg formájában történik, a fogadónak ismernie kell az ehhez használt jelkészletet, azaz betűket. Az ethernet kártya

példáját továbbgondolva: nem elegendő az a tény, hogy a kártya és a hálózat egyformán 100 Mbit/s sebességű, óhatatlanul szükséges további feltétel, hogy a hálózaton szabványos ethernet-keretek közlekedjenek, különben a kártya nem tud mit kezdeni a jelekkel.

A negyedik lépcsőfok a **megértés**. Nem elegendő a jeleket ismerni, ismerni kell azt a nyelvet is, amelyen az üzenetet közlik. A számítástechnikai példát továbbgondolva: szükséges egy olyan program, amely a kártya által „elfogott" keret tartalmával valamit tud kezdeni. Hiába küldünk egy adott IP-címre HTTP GET kérést, ha az adott gépen nincs webkiszolgáló program, amely valamit kezdeni tudna vele.[3]

Ha mind a négy lépés sikeres volt, akkor mondhatjuk, hogy a fogadó számára rendelkezésre áll az az *adat,* amelyet a küldő vele tudatni szándékozott. Hogy ebből az adatból lesz-e *információ,* az már egy másik kérdés, azon múlik, hogy a fogadó azt tudja-e és akarja-e értelmezni.

Mindez azért fontos, mert az ismeretet időben, megfelelő, a fogadónak testre szabott formában, számára érthetően: érthető jelekkel és érthető nyelven kell közölni. Természetesen az ismeretet hordozó közeg sajátosságait, saját szabályait sem lehet figyelmen kívül hagyni. Mivel a legtöbb esetben az ismerethordozó közeg a nyelv, ezért különösen illik odafigyelni annak szabályaira, azok maradéktalan betartására is.

2.3 Adatvédelem és adatbiztonság

Az adatvédelem kifejezés puszta jelentése alapján úgy vélhetnénk, hogy az adatvédelem fogalmába beletartozik minden olyan dolog és tevékenység, amely adatainkat megvédi a káros behatásoktól. Az „adatvédelem" kifejezést azonban elsődlegesen a jog használja, l. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt, amely az 1992. évi LXIII. törvényt – az Adatvédelmi törvényt – váltotta 2012. január 1-től. Így tehát adataink nem jogi, hanem technikai értelemben vett megvédését nem nevezzük adatvédelemnek, hanem inkább adatbiztonságról beszélünk. Az adatvédelem kifejezés elsősorban a személyes adatoknak a jogi védelmét jelenti az illetéktelenek általi megismeréstől és/vagy kezeléstől.

2.4 A valós és virtuális világ

Szokás a számítógépek és a számítógépes hálózatok világát virtuális világnak, virtuális valóságnak nevezni, megkülönböztetendő a hagyományos valóságtól és világtól. Megvan ennek az alapja, mert komoly, és komoly következményekkel

[3] L. pl. a Nightwish elhíresült számát a „finn-magyar nyelvrokonságról", http://www.youtube.com/watch?v=Otcj0rLZpYc

járó különbségek vannak a „két világ” között. Nézzünk erre egy szemléletes példát.

Ha ellopják a kocsimat, azt elég hamar és egyértelműen fölfedezem, egyszerűen abból a körülményből, hogy nincs ott, ahol hagytam. A tétel megfordítása is igaz, ha a kocsim ott van, akkor nem lopták el. Ugyanez az adatokra már nem igaz. Attól, hogy adataim eredeti helyükön megvannak, nem következik, hogy senki más nem fért hozzájuk, nem nézett bele, nem másolta le. A másik különbség, hogy kocsilopás esetén a tettes a tett időpontjában ott van a tett helyszínén. Adatlopáskor (vagy egyéb „virtuális útonálláskor”) a tettesnek nem feltétlenül kell ott lennie az adatok tárolási helyénél, sőt egyáltalán nincs olyan kitüntetett hely, ahol muszáj lenne tartózkodnia. Mi több, sem a tett időpontjában (sem semmikor máskor) nem muszáj adott helyen tartózkodnia. Belátható, hogy ilyen világban nemcsak az esetleges tettes utólagos elkapása és felelősségre vonása nehéz, de a nemkívánatos tettek megelőzése sem könnyű.

Vegyük ehhez hozzá, hogy az adatok, mint a „virtuális világ elemei” nagyon is fizikai hordozókon – és csak azokon – léteznek. A fizikai hordozónak pedig csekély mértékű, részleges meghibásodása is a teljes adatmennyiség azonnali elvesztését jelentheti. Mindezek merőben új és szokatlan jelenségek, összehasonlítva a korunkat megelőző, több évezredes megszokásokkal, hagyományokkal. Ilyen körülmények között kellene az adatok biztonságáról beszélni, azt meghatározni (és persze biztosítani).

Van öt, ún. alapkövetelmény, amelyek teljesülése az üzemszerű használhatóság előfeltétele:

- rendelkezésre állás, elérhetőség a jogosultaknak
- sértetlenség (sérthetetlenség, valódiság)
- jellegtől függő bizalmas kezelés
- hitelesség
- a teljes információs rendszer működőképessége

Az ezen öt alapkövetelményt fenyegető tényezők eredőjét nevezzük alapfenyegetettségnek. Ez alapján úgy lehet meghatározni az **informatikai biztonság** fogalmát, hogy az akkor áll fenn, ha a(z információs) rendszer védelme az alapkövetelmények szempontjából zárt, teljes körű, folyamatos és kockázatarányos.

Zárt: minden fontos fenyegetést figyelembe vesz.

Teljes körű: a rendszer összes elemére kiterjed.

Folyamatos: az időben változó körülmények ellenére is megszakítás nélküli.

Kockázatarányos: a feltehető kárérték és a kár valószínűségének szorzata nem haladhat meg egy előre rögzített küszöbértéket. Ez a küszöbérték üzleti döntés

eredménye.

Az ezen értelemben vett informatikai biztonság elérése és fenntartása a fizikai, ügyviteli és algoritmusos védelem[4] megfelelő, együttes alkalmazásával lehetséges.

Nagyon fontos tudatosítanunk, hogy nincs, nem létezik 100%-os biztonság, nemcsak az informatikában, számítástechnikában, de az élet egyetlen területén sem. Lehet közelíteni hozzá (egyre nagyobb ráfordítással), de elérni sosem lehet, mindig van egy maradványkockázat. Ellenben eleinte a szerény mértékű ráfordítás is jelentős mértékű biztonságnövekedést eredményez. Az elérhető, illetve elért szintjét a biztonságnak sok tényező eredője határozza meg. Mint az élet egyéb területein általában, itt is a leggyöngébb láncszem az ember.

3 Veszélyek

3.1 Hardver, szoftver, adat

A számítógépes környezet három fő, logikai szintű eleme a hardver, a szoftver és az adatok. Ebből nyilvánvalóan a legértékesebb (sőt az egyetlen igazán értékes) az adat. A hardver pótolható, boltból beszerezhető, pénzért megvásárolható. A szoftverre ugyanez vonatkozik. Evvel ellentétben ha a munkánk eredményeképpen keletkezett adatokat elveszítjük, azok pótlása nem ilyen egyszerű. Vannak olyan adatok, amelyek pótolhatók: ha adott munkamennyiséget újból elvégzünk, vagy elvégeztetünk, az adatok újra előállíthatók. Például ha a gépi könyvelés adatai elvesznek, a hiteles, papírbizonylatok adatait újból gépre lehet vinni, és a gépi könyvelést lehet folytatni. Vannak azonban újra elő nem állítható (=pótolhatatlan) adatok is: a webáruházba beérkezett, nyugtázott, de még föl nem dolgozott megrendeléseket aligha lehet újra begyűjteni, az elmúlt év időjárási mérési adatait is lehetetlen újból megmérni.

Éppen ezért elsődlegesen és leginkább az adatainkra kell vigyáznunk.

3.2 „Vírusok”

A számítógépes vírusok nevüket a biológiai vírusokról kapták, azon tulajdonságuk alapján, hogy képesek „szaporodni”, pontosabban önmagukat terjeszteni, így számukat gyarapítani. Az elmúlt mintegy negyed században nemcsak a számítástechnika általában, de a „vírusok” is jelentős fejlődésen mentek keresztül, számos olyan „kártevő” programfajta bukkant föl, amelyre nem feltétlenül illik rá az eredeti ismérv (önmaga többszörözése), mégis a köznapi szóhasználatban a vírusok közé soroljuk őket. Ennek pedig az az alapja, hogy hatásukban,

[4] L. a Védelem c. fejezetet

szerepükben nincs érdemi különbség: kárt okoznak vagy okozhatnak a rendszer működésében, növelik a kockázatot, erőforrásokat kötnek le, emésztenek föl fölöslegesen.

Közelebb jutunk a lényeghez, ha ezt a kibővített értelmezést úgy próbáljuk meghatározni, hogy „vírus"-nak tekintünk minden olyan programot vagy számítástechnikai jelenséget, amely a rendszer gazdájának tudta nélkül, akarata ellenére és érdekeit sértve működik. Helyesebb és pontosabb lenne a „rosszindulatú számítástechnikai program vagy jelenség" kifejezés, amelynek a hagyományos értelemben vett vírus valódi részhalmaza, de mit tegyünk, ha nyelvünkben nem így honosodott meg. Védekezni mindenképpen kell ellenük.

Ezen károkozókat számos módon lehet csoportosítani, például történetiség, terjedésmód, károkozás típusa stb. alapján. Nagyon vázlatos áttekintést nyújtva nagyjából az időrendiség alapján a következő fejlődési vonalat ábrázolhatjuk:

Klasszikus programvírusok: a személyi számítógépek és a DOS végrehajtható programállományait használták „gazdaállat"-ként, a COM és EXE fájlok végéhez fűzték hozzá saját kódjukat, a program elejét úgy módosítva, hogy a program futtatásakor előbb a végéhez fűzött kártékony kód fusson le, amely aztán helyreállította a program elejét, és visszaadta oda a vezérlést. A kártékony kód alapvetően két fő részből áll: továbbmásolta magát néhány, még nem fertőzött program végére, illetve adott feltétel teljesülése esetén (pl. péntek 13-án) végrehajtotta eredeti célját. A hatékony terjedési közeget az biztosította, hogy ekkoriban az elsődleges adathordozó eszköz az írható-olvasható hajlékonylemez volt.

Boot vírusok: a rendszerindítás folyamatát, az operációs rendszer betöltő programját módosítja, azaz még azelőtt lép működésbe, hogy az operációs rendszer elindult volna, és az esetleges vírusvédelem működni kezdene.

Makróvírusok: az idő múltával a telepítőkészleteket egyre inkább CD-n adták ki, a hajlékonylemezek egyre inkább kiszorultak, a közönséges gépközi adatcsere feladata maradt meg számukra. Evvel párhuzamosan egyre általánosabbá vált a személyi számítógépek irodai használata, a DOC és XLS állományokat egyre nagyobb arányban vitték egyik gépről a másikra. A Microsoft Word fejlett, sőt talán túl fejlett makrózási[5] lehetőségekkel bírt. Makróvírus jelenlétét a legkönnyebben és legbiztosabban arról lehetett megállapítani, hogy az Eszközök menüből eltűnt a Makrók menüpont – a makróvírus átdefiniálta a menüt, elemi önvédelemből.

A makróvírusok után a helyzet bonyolultabbá vált, egyre kevésbé különülnek el határozott fázisok. Mindenképpen említendő csoportok az alábbiak.

Email vírusok vagy script vírusok: ahogy az elektronikus levelezésben elterjedt a

[5] A makró parancsok és utasítások sorozata, amelyeket egy konkrét művelet automatikus végrehajtására egyetlen paranccsá fűz össze. http://office.microsoft.com

html formátum a csupasz szöveg mellett, majd egyre inkább helyett, lehetővé vált a html-be ágyazott JavaScriptek, illetve VisualBasic Scriptek alkalmazása. Ekkor dőlt meg az a korábbi állítás, miszerint egy email puszta elolvasása nem okozhat problémát. A VBS csoport „szép" példája a Kurnyikova-vírus.

Hálózati férgek: számítógépes hálózaton terjednek, az operációs rendszer hibáinak, biztonsági réseinek kihasználásával, nincs szükségük hordozóprogramra.

Trójai programok: ezek már nem vírusok a klasszikus, szűk értelemben véve. Olyan, hasznosnak látszó program, amely a felhasználó számára ismeretlen, szándékaival és érdekeivel ellentétes hatású részt, funkciót is tartalmaz. Ennélfogva terjedési, pontosabban terjesztési módjaik a lehető legváltozatosabbak. Tipikusnak mondható, amikor a népszerű, többé-kevésbé drága programot ingyenesen lehet megszerezni, letölteni – csakhogy nem az eredeti állapotában, hanem a közzétevő által módosítottan.

Egyebek: ide sorolhatók olyan egyéb kártékony programok, amelyek a fenti csoportosításba nem illenek bele, és többnyire a félrevezetett felhasználó közreműködésével lépnek működésbe. Például kap a felhasználó egy emailt látszólag valamelyik ismerősétől, amelyben felhívják figyelmét egy honlapra, és a mellékletben ott is szerepel a www.valami.com. A felhasználó pedig ösztönösen kattint rá, nem gondolván végig, hogy *link* nem lehet *csatolmány,* link csak a levél törzsében érkezhetne. A .com (dotcom) a leggyakoribb legfelső szintű névvégződésként ismeretes mostanában, ha azonban csatolt állományként érkezik, akkor egy COM típusú, futtatható gépi kódot tartalmazó állományról van szó.

A **víruskeresés és vírusirtás** elég hamar külön iparággá nőtte ki magát. A víruskeresési eljárások alapvetően két fő csoportba tartozhatnak. Kártékony programokat lehet keresni jellegzetes, csak rájuk jellemző, adatbázisba foglalt bájtsorozatok alapján. Másik lehetőség a heurisztikus keresés, amikor nem konkrét bájtsorozatokat keresünk, hanem a meglévő programokat elemezzük, hogy találunk-e bennük olyan jellegzetes megoldásokat, amelyek rosszindulatú kódra utalnak.

Nyilvánvaló, hogy az első megoldás a vírusok után kullog, azaz egy új vírusnak előbb el kell terjednie annyira, hogy valaki fölfigyeljen rá, majd a víruskeresők fejlesztői elemzik azt, majd végül a rá jellemző bájtsorozat bekerül az adatbázisba. Addig azonban órák, napok telnek el, és nincs orvosság. A második megoldás megtalálhatja a még ismeretlen, új kártevőket is, viszont nincs biztosíték arra, hogy *minden* rosszindulatú kódot, kódrészletet helyesen felismer. Emellett sajnos másra sincs biztosítékunk, amint azt az alábbi eset mutatja.

A **Sony rootkit** példája. 2005 őszén robbant ki a botrány: a Sony zenei CD-ire a zene mellé egy olyan szoftvert tett, amely, ha a felhasználó számítógépén hallgatja a CD-t, telepít egy rejtett kémprogramot a felhasználó gépére, amely titokban adatokat küldött a Sonynak. Ha ezt egy hacker teszi, akkor bűncselekményt követ el. Az igazi probléma esetünkben azonban nem az, hogy vannak a többieknél

egyenlőbbek, hanem az, hogy mintegy másfél év alatt egyetlen víruskereső program sem vette észre, és nem jelezte a betolakodót. A botrány kirobbanása után is csak lassan és hiányosan reagáltak: eleinte csak az álcázást távolították el a Sony feltelepült kémprogramjáról, magát a kémprogramot nem. „Mi történik akkor, ha a rosszindulatú szoftverek alkotói összejátszanak azokkal a vállalatokkal, amelyeket pont azért fizetünk, hogy megvédjenek bennünket ezektől a rosszindulatú programoktól?”[6]

Spam, kéretlen reklámlevél. Annyiban tartozik ide, hogy igen jelentős erőforrásokat emészthet föl. Becslések szerint a spam aránya az összes email 70-90% is lehet. Ez önmagában nagyon megterheli a hálózati erőforrásokat, és megterhelné a felhasználók munkaidejét és idegrendszerét is, ha jobb rendszergazdák nem szűrnék ki igen hatékonyan a kéretlen levelek döntő többségét – ismét csak jelentős erőforrások fölemésztésével.

3.3 Motiváció, emberi tényező

A bevezetőben röviden szó esett arról, hogy tényleg az információs társadalom korát éljük, a digitálisan tárolt és kezelt adatok szerepe, mennyisége és a hétköznapi élet számos területének az azoktól való függésének mértéke folyamatosan növekszik. Lehetne erre azt felelni, hogy én/mi túl kis halak vagyunk ahhoz, hogy bárki érdeklődését felkeltsük, de ez nem volna igaz. Vegyünk néhány lehetséges indítékot, csak illusztrációként.

Tipikus motivációs tényező lehet a szakmai kivagyiság, dicsekvés, az „én még ezt is meg tudom tenni” indíték. Ez párosulhat politikai figyelemfelkeltő akciókkal is (a magyar alkotmány szövegének módosítása az Alkotmánybíróság honlapján pl.). Természetesen egy kisvállalkozás esetében talán nem túl valószínű, hogy pont ezen indítékok miatt intézzenek számítógépes rendszere ellen bármiféle támadást. Az azonban sokkal elképzelhetőbb, hogy egy elbocsátott dolgozó megpróbál revansot venni a vállalaton a személyén esett, jogtalannak érzett sérelem miatt.

Ha rendszerezni próbálunk, három fő csoportba sorolhatjuk azon okokat, veszélyeket, amelyek adatainkat – így vagy úgy – fenyegethetik. Egyrészt adataink elveszhetnek anélkül, hogy emögött bármiféle személyes vagy általános rosszindulat állna. Másfelől áldozatául eshetünk általános jellegű (értsd: nem személy szerint ellenünk irányuló) támadásnak, ennek is két válfaja van: a minél több számítógépet begyűjteni kívánó botnet építés, illetve az egyéb illegális tevékenység leplezésére szolgáló közbülső gépek megszerzése. Harmadrészt pedig nem szabad elfelejtkezni a személyesen ellenünk (magánszemély vagy vállalat) irányuló támadás lehetőségéről sem, legyen a mögöttes szándék akár bosszúállás, akár anyagi haszonszerzés, akár féltékenység.

Mi az a botnet? A botnet (robot network) olyan számítógépek összessége,

[6] Schneier, 2010. pp. 266-269.

amelyeken valamilyen módon – többnyire az operációs rendszer vagy valamelyik tipikus alkalmazás, esetleg a felhasználó hibáját kihasználva – sikerült bejuttatni egy olyan programot, amely lehetővé teszi más számára, hogy a számítógépet gazdája tudta nélkül, annak akarata és szándéka ellenére használni tudja. Tipikus alkalmazási terület a kéretlen reklámlevelek (spam) küldése: nagy mennyiségű reklámlevelet nagy mennyiségű, ún. zombigép felhasználásával lehet rövid idő alatt kiküldeni.

Illegális tevékenység leplezéséhez célszerű közbülső számítógépeket használni a nyomok elrejtése céljából. Azaz, hogy ha a tevékenység és az elkövető megállapítására nyomozás indul, akkor az legfönnebb a közbülső számítógépet, vagy azok egy részét találja csak meg (ha egyáltalán).

Mindkét esetben (az elsőben talán kevésbé, a másodikban jelentősen) növekszik annak veszélye, hogy adataink is áldozatul esnek. Nemcsak azért, mert ismeretlen programok működése eleve kockázattal jár, hanem – főként a második esetben – az elkövető saját nyomainak eltüntetése céljából a felhasznált számítógépet olyan állapotba hozhatja, hogy gazdája kénytelen legyen azt újratelepíteni. Ha valaki a mi gépünk közbeiktatásával törte föl a CIA honlapját, nem fog azon tanakodni, hogy voltak-e pótolhatatlan adataink a gépünkön...

Ezen esetek hasonlítanak az általános célú gépkocsilopáshoz: a keresett típusú kocsik közül azokat fogják nagyobb valószínűséggel ellopni, amelyek a többihez képest kevesebb, vagy egyszerűbb védelemmel vannak ellátva. Nagyobb eséllyel válik gépünk zombivá, vagy használják ugródeszkaként törvényellenes cselekményekhez, ha még az általánosan ismert és elvárható védelemmel (tűzfal, vírusirtó, programfrissítések) sincsenek ellátva.

A személyre szabott, célzott támadás ahhoz hasonlítható, ha különleges, egyedi kocsink van, és a „gépkocsitulajdon átruházó törvénytelen társaság” pont ilyenre kapott megrendelést. Ha ilyen kocsi birtokában azt észleljük, hogy követnek, figyelnek, csak egyet tehetünk: meg kell próbálni a kocsit még azelőtt eladni, hogy ellopnák. Számítógépes környezetben ennek az felel meg, hogy – elegendő motiváció és erőforrás birtokában – bármely rendszer sebezhető. A Stuxnet vírus úgy pusztított az iráni atomlétesítményekben, hogy azok számítógépei egyáltalán nem kapcsolódtak az internetre...

Nem szabad említés nélkül hagyni az emberi tényezőket sem. A facebook-ot előszeretettel használják már nemcsak arra, hogy a leendő munkatársról előzetesen megpróbálják megtudni, vajon beleillik-e majd a vállalat és a kollektíva körébe, de betörők is arra (a Google StreetView és a Google Maps kiegészítésével), hogy hol érdemes próbálkozni. Ezen túl pedig – sajnos – általános tapasztalat, hogy aki az emberi hanyagságra, gondatlanságra, nemtörődömségre és tudatlanságra alapít, előbb-utóbb megtalálja számítását. Ezen módszer tudományos elnevezése a „social engineering” vagy „social hacking”, amikor is a „süket duma” eszközével veszik rá az áldozatot olyan adatok kiadására, amelyeket jobb lett volna nem megadnia. Ennek rokon területe, amikor ügyes látszatkeltéssel egyszerűen sikerül

rávenni a felhasználókat egyetlen – meggondolatlan – egérkattintásra, vagy akár közvetlenül becsapni őt.

4 Adatvesztés, -sérülés ellen

4.1 Kiváltó okok

Adataink megsérülése, részleges vagy teljes megsemmisülése, eltűnése számos okból bekövetkezhet. A teljesség igénye nélkül néhány: természetes tönkremenetel, elemi kár (tűz, árvíz, árvíz, földrengés, csőtörés, tűzoltás járulékos hatása, villámcsapás másodlagos hatása, eszközlopás (hardver eladása céljából vagy magának az adattartalomnak a megszerzésére), szoftverhiba, rövidzárlat, emberi hiba, „vírus" stb.

Ezek közül a természetes tönkremenetelt emelném ki. Nincs olyan háttértár manapság, amely garantálná az adatok olvasható állapotban való megőrzését, akár csak határidőn belül. Valamennyien találkoztunk már olvashatatlanná vált írt CD/DVD-vel. A memóriakártyák véges sok írási műveletet bírnak ki felépítésükből adódóan (ha ezek az írási műveletek sűrűn követik egymást, akkor ez a szám még jelentősen csökkenhet is). A mágnesszalag esetén a természetes lemágnesedőzési folyamat mellett az ismételt rugalmas alakváltozás és mechanikai igénybevétel is növeli az élettartam bizonytalanságát. A merevlemezek pedig olyannyira precíziós finommechanikai eszközök (10.000 fordulat/perc, az adathordozó felület és az író-olvasó fej távolsága nanométer nagyságrendű), hogy egészen kis behatás is tönkremenetelt eredményezhet.

4.2 Mit tehetünk ellene?

Eső után köpönyeg: ha bekövetkezett a katasztrófa, és adataink elvesztek, a sérült adathordozókról történő adatmentés nemzetközi hírű magyar vállalkozása, a Kürt Rt.[7] lehet a segítségünkre. Ha ezt szeretnénk elkerülni, vagy legalábbis csökkenteni a valószínűségét, három dolgot lehet, illetve kell tennünk, ebben a fontossági sorrendben: biztonsági mentés, védelem, éberség.

4.2.1 Biztonsági mentés

Egy mondás szerint az adatokból egy példány nem példány. Két példány fél példány, három példány a példány, négynél kezdődik a biztonság. Kicsit komolyabban: elemi és elsődleges érdekünk, hogy fontos adatainkból legyen naprakész biztonsági másolatunk. Így bármilyen okból bekövetkező adatvesztés

[7] http://kurt.hu/

esetén az eredeti állapotot helyre tudjuk állítani (az esetleges hardver-, ill. szoftverhiba kiküszöbölése után).

A mentési eljárás kialakításának legfontosabb szempontjai a következők:

- adatok mennyisége: egészen más eljárásokat alkalmazhatunk egy egyetemi hallgató néhány száz megabájt adatot tartalmazó munkaterülete esetében, mint egy nagyvállalat kritikus fontosságú, esetleg több terabájtos adatbázisa esetében.
- adatok változékonysága: nem mindegy, hogy az adatok mekkora hányada milyen gyakorisággal változik, illetve hogy könyvtárstruktúrába rendezett fájlokat kell menteni, vagy pedig (működő) adatbázist – alapvetően befolyásolja az inkrementális, ill. differenciális mentés lehetőségeit.
- helyreállítás időigénye: mérlegelni kell, hogy egy esetleges üzemzavar esetén mennyi időnk van az eredeti, működő állapot helyreállítására – akár két nap, vagy pedig minden körülmények között biztosítani kell a folyamatos üzemet.
- távoli helyszín: a biztonsági mentés helyszínének mindig fizikailag távol kell lennie az üzemi helyszíntől, hogy akár természeti katasztrófa esetén is megmaradjon a biztonsági mentés, ezen túl megfontolandó lehet a példányok számának növelése is.
- változatok száma: a több, korábbi állapot megőrzése az egyetlen lehetőség a logikai természetű hibák (pl. dokumentum tartalmának részleges véletlen törlése) ellen.

Vegyünk egy példát. Adott egy egyetemista, aki szakdolgozatát készíti. Dolgozik magán az anyagon, a szakdolgozat.doc fájl állandóan változik, emellett anyagokat is gyűjt az internetről. A teljes adatmennyiség nagyjából 2-300 MB. Célszerű és hatékony megközelítés, ha egy pendrive-ra készíti a biztonsági mentéseket, a napi munka végeztével, oly módon, hogy az aznapi dátumról elnevezett alkönyvtárba másolja mindazon fájlokat, amelyek a megelőző mentés óta keletkeztek, vagy megváltoztak (dátum vagy archív bit alapján).

4.2.2 Védelem

Ahhoz, hogy adataink védelme hatékony lehessen, három különböző síkon együttesen kell gondolkodnunk – és persze cselekednünk. Ezek a fizikai, az ügyviteli és az algoritmusos védelmi síkok (vö. informatikai biztonság fogalmával). Az egyenszilárdságú és eredményes védelem előfeltétele, hogy annak mindhárom síkra ki kell terjednie.

A **fizikai sík** két lényegi dolgot takar. Egyrészt biztosítani kell az optimális, de legalább a még elfogadható üzemi körülményeket (hőmérséklet, páratartalom, por, tartalék alkatrészek stb.), másrészt pedig a szükséges vagyonvédelmi

intézkedésekről sem szabad elfelejtkezni.

Az **ügyviteli sík** a folyamatok szabályozásának, a szabályzatoknak a síkja. A fizikai sík önmagában ugyanis nem elegendő. Egy példával élve: hiába zárjuk be a szerverszoba ajtaját, ha a portás beengedi azt, aki egy szerszámos táskával érkezvén arról tájékoztatja pl., hogy „...a művektől küldték, mert szóltak, hogy zsírozni kell a switcheket, mert a blűzni nem jól adja le a szikrát" (social hacking/engineering, „süket duma" eszköze). Azaz: szükséges pontosan szabályozni, hogy ki, mikor, mit és hogyan tehet meg, illetve nem tehet meg. Szükség van informatikai biztonsági szabályzatra (is), amely mindezt egységes módon áttekinti.

Minél nagyobb, bonyolultabb felépítésű egy vállalat, illetve annak információs rendszere, annál lényegesebb, hogy a felhasználók azonosítása és rendszerhasználatuk nyomon követése ne áttekinthetetlen, ad-hoc jellegű legyen. Megfelelő felhasználómenedzselési rendet kell kialakítani, hogy a felhasználók, hozzáférési jogosultságaik, munkájukból adódó szerepköreik kezelése összhangban legyen, mégpedig naprakészen. Mert ha egy új dolgozó a munkájához szükséges hozzáféréseket, jogosultságokat késve kapja meg, hát annyi baj legyen, néhány órával, esetleg egy nappal később kezdi az érdemi munkát. De ha a kilépett, elbocsátott dolgozó jogosultságait két nappal később vonják vissza (vagy egyáltalán nem), az esetleg beláthatatlan következményekkel járhat.

Egyes vállalatoknál előírás az „üres asztal, fekete képernyő", ami azt jelenti, hogy semmilyen dokumentumot, sem papíralapút, sem elektronikusat, nem szabad elöl hagyni, sem a fizikai, sem a virtuális „asztalon", nehogy illetéktelenek abba belepillanthassanak.

A szabályzatok kapcsán fel kell hívni a figyelmet egy újfajta veszélyre: a tartalmi lényeg helyett a különféle szabványoknak, előírásoknak való formális megfelelőségek előnyben részesítése (a személyes felelősség csökkentése érdekében). A másik lehetséges probléma pedig abból a régóta közismert körülményből adódik, hogy minden szabály annyit ér, amennyire azt betartják, betartatják.

Az **algoritmusos sík** arra a gondolatra épül, hogy célszerűen magát a számítógépet is használjuk fel önmaga és társai védelmére. Olyan elemek tartoznak ide, mint a víruskeresők alkalmazása, megfelelően beállított tűzfalak, frissítések, naplózás, naplóelemzés, felhasználó-menedzsment (l. ügyviteli sík) és jogosultságkezelés stb.

A *víruskeresők* a mai világban nélkülözhetetlenek. Fontos, hogy naprakész vírusadatbázis alapján működjenek, és a vírusadatbázis frissítésének lépését a felhasználó ne léphesse át. Emellett nem árt tudatosítani, hogy *nem* nyújtanak teljes körű, garantált védelmet (l. a „Vírusok" c. részt).

A *tűzfal* az adatforgalom szabályozásával próbálja védeni az egyes

számítógépeket, illetve hálózati szegmenseket a nemkívánatos behatolásoktól, illetve ilyen kísérletektől, illetve a nemkívánatos kifelé menő adatszivárgástól. Megfelelő beállítása, még inkább megtervezése komoly szakértelmet és a helyi sajátosságok alapos ismeretét igényli.

A *naplózás* során a számítógép naplószerűen feljegyzi bizonyos események megtörténtét. Célja az, hogy rendkívüli esemény bekövetkezése esetén legalább utólag esélyünk legyen annak megállapítására, hogy mi (és esetleg miért, hogyan) is történt. Ettől nem elválasztható a *naplóelemzés.* A naplóelemzés célja az, hogy egyes nemkívánatos eseményeket előre lehessen jelezni, valószínűsíteni.

Ilyen lehetőség – például – ha előre meg tudjuk állapítani, hogy valamelyik merevlemez cserére szorul, mert küszöbön áll a meghibásodása. A ma forgalomban lévő SATA és SCSI merevlemezek komoly beépített öndiagnosztikával rendelkeznek. A megfelelő segédprogrammal ezt a belső tesztet el lehet indítani, majd annak eredményét lekérdezni, és megvizsgálni. Egyes esetekben (nem mindig!) ezen eredmények (pl. hibás szektorok számának növekedése) jelzik, hogy a lemezegység meghibásodása közeleg, így lehetőségünk van a tervezett cserére, nem következik be a váratlan rendszerleállás.

4.2.3 Éberség

A különféle szabályok mechanikus meg-, és betartása önmagában nem mindig elegendő. Mindig adódhatnak olyan váratlan helyzetek, események, amikor a józan eszünket kell (kellett volna;) használnunk. Ha például egy felsőoktatási intézményben hónapokon keresztül nincs tanúsítványa a Neptun-kiszolgálónak, a hallgatók és az oktatók hozzászoknak ahhoz, hogy a böngésző erre vonatkozó figyelmeztető ablakát reflexszerűen bezárják és továbblépjenek. Ebben az esetben azonban nem lehet kizárni egy közbeékelődéses támadás lehetőségét, amelyre kiváló lélektani lehetőséget adna egy ilyen helyzet. Ilyen helyzetben a diák és az oktató akkor jár el körültekintően, ha legalább telefonon ellenőrzi a tanúsítvány ujjlenyomatát (fingerprint).

De ki gondolna arra, hogy az intézményen belüli dohányzási tilalomnak is vannak adatbiztonsági hatásai? Ha a dolgozók az épület előtt, az utcán dohányoznak, és közben fontos és kényes dolgokról beszélgetnek, azt nagyon könnyű pl. a szemközti épületből lehallgatni...

És végül, de nem utolsósorban: fel kell ismerni, és nem szabad bedőlni a „nagy süket duma”, a social engineering eszközének. Kevin Mitnick, napjaink egyik leghíresebb hackere számos eredményét nem elsősorban számítástechnikai szakismeretekkel, hanem ügyes rábeszéléssel érte el.

4.3 Felhasználók azonosítási módjai

A felhasználók gépi úton történő azonosítása az egyik leggyakoribb tevékenység,

jelentőségét tekintve kritikus fontosságú művelet. Idők folyamán számos technikai megoldása alakult ki. Ezeket három fő csoportba tudjuk besorolni: ezek a tudás alapú, a birtoklás alapú és a biometrikus azonosítási módszerek. Mindegyik fajtának megvannak a maga előnyei és hátrányai, és természetesen igen különböző mértékű árai.

4.3.1 Tudás alapú

A tudás alapú azonosítás arra épül, hogy csak az adott felhasználó ismerhet valamilyen adatot. Tipikus példa erre a különféle jelszavak, PIN-kódok alkalmazása. Előnye, hogy igen egyszerű megvalósítani, igen olcsó, hiszen semmilyen külön eszközt, felszerelést nem igényel, és egyértelmű (igen vagy nem) választ ad. Hátránya, hogy egyes esetekben illetéktelen személy is sikeresen megtippelheti, illetve valamilyen más módon megtudhatja. Bővebben l. a „Jó jelszó" c. részben. Mindenképpen szükséges elem, hogy az illetéktelen próbálgatásokat megnehezítsük, gyakorlatilag lehetetlenné tegyük. Ezt a célt szolgálja például az, hogy egy bankkártya PIN-kódjának harmadszori sikertelen tippje a kártya felfüggesztését váltja ki.

4.3.2 Birtoklás alapú

A birtoklás alapú azonosítás arra épül, hogy a felhasználó (és csak ő) birtokol valamit, legyen ez egy intelligens kártya (smart card), egy RFID-eszköz („flepni"), vagy akár egy mobiltelefon, pontosabban annak SIM-kártyája. Tipikus alkalmazás területe az internet-bankolás esete: a jelszó alapú azonosítást követő lépésben néhány percen belül meg kell adni egy számkódot, amelyet SMS-ben küld ki a rendszer a bejegyzett mobilszámra. Előnye, hogy a felhasználótól nem várja el egy „enpluszegyedik" jelszó megjegyzését, és ellenőrzése a jelszóhoz hasonlóan nagyon egyszerű, és ugyancsak egyértelmű. Hátránya viszont, hogy az azonosítás alapját jelentő birtokolt tárgyat általában elő kell állítani, ami több-kevesebb pénzbe kerül. Probléma, hogy a tárgyat el lehet lopni, ami nem feltétlenül tűnik fel azonnal a jogos tulajdonosnak, egyes esetekben azt annak tudta nélkül, esetleg távolról is le lehet másolni.

4.3.3 Biometrikus

A biometrikus azonosítás a felhasználók egyedi biológiai jellemzőin alapul. Beszélhetünk felismerésről, illetve ellenőrzésről. A felismerés az, amikor a biometrikus jellemző alapján megállapítja a rendszer a személy kilétét („ennek az arcképnek a gazdája X. Y."). Az ellenőrzés egyszerűbb feladat, ennek során a felhasználó valamilyen formában, pl. egy kártya lehúzásával azt állítja, hogy ő X. Y., majd a rendszer ellenőrzi, hogy vizsgált biometrikus jellemzője (pl. arcképe) megfelel-e az adott felhasználó adott biometrikus jellemzője tárolt adatainak. Vitathatatlan előnye, hogy sem megjegyezni nem szükséges semmit, sem tárgyat nem kell hurcolni, a biometrikus jellemző állandóan „kéznél" van. A közhiedelem szerint a biometrikus jellemzőt hamisítani sem lehet.

A módszer hátránya, hogy a biometrikus azonosítás v. felismerés igen bonyolult algoritmusokon alapul, és az eredménye nem egyértelmű igen vagy nem, hanem egy valószínűség. Evvel van összefüggésben a biometrikus módszerek minőségének két alapvető mutatója, a fals pozitív és fals negatív azonosítások mutatószáma, az FAR és az FRR (False Accept Rate, False Reject Rate), amelyek azt mutatják meg, hogy milyen valószínűséggel fog a rendszer tévesen elfogadni egy jogosulatlan próbálkozót, illetve elutasítani egy egyébként jogos felhasználót. A két mutatószám között összefüggés van: ha a rendszer hangolásával az egyiket csökkentik, az a másik növekedését eredményezi.

További problémák, hogy a vizsgálat tárgyát képező biometrikus jellemző baleset következtében időlegesen vagy maradandóan értékelhetetlenné válik. Másik probléma, hogy a módszerhez különleges érzékelő egységekre van szükség (ujjnyom-olvasó, retinaszkenner stb.), amelyek ára esetenként jelentős is lehet, illetve hogy ezen eszközökhöz az esetlegesen ellenérdekelt felhasználó fizikailag hozzáfér, megpróbálhatja magát az eszközt manipulálni. Az sem feltétlenül igaz, hogy biometrikus jellemzőt nem lehet manipulálni.[8] Ezen kívül fölmerül a magánszféra védelmének kérdése is: nem biztos, hogy mindenki szívesen beleegyezik, hogy biometrikus jellemző adatait kezeljék.

Ne felejtkezzünk meg azonban a legkézenfekvőbb biometrikus azonosítási lehetőségről, ez pedig a portás.

4.4 Jelszavak

A felhasználók azonosítási lehetőségei közül ragadjuk ki a legegyszerűbb és legkézenfekvőbb lehetőséget, a jelszavas azonosítást. Mivel nemcsak a legegyszerűbb és legkézenfekvőbb megoldás, hanem a leggyakoribb is (nem véletlenül), érdemes közelebbről megvizsgálni. Van néhány olyan – egyszerű – szabály, amelyek betartása jelentősen megnöveli a jelszavas azonosítás biztonságát, illetve amelyek figyelmen kívül hagyása rendkívüli módon megnöveli annak valószínűségét, hogy azt előbb-utóbb valaki ki fogja játszani, és így illetéktelenül megszerzi a védett hozzáférést.

4.4.1 Jó jelszó

Általános téveszme, hogy a „jó” jelszó valami ilyesmi: „zMP#x14!”, azaz valami olyasmi, ami kis- és nagybetűket, számjegyeket és írásjeleket is kell tartalmazzon, és teljesen értelmetlen. Ha efféle jelszavakra kényszerítjük rá dolgozóinkat, annak csak egy eredménye lehet, megjelennek a sárga öntapadós cetlik a monitor szélén (jobb esetben kevésbé szem előtti helyen).

A hétköznapi gyakorlat sajnos pont a másik végletet mutatja. Egy konkrét

[8] L. pl. Tsutomu Matsumoto et al., 2002.

elemzés[9] szerint „a legtöbbet használt 25 jelszó között 174-szer fordult elő magyar keresztnév vagy becenév, további 385 esetben pedig valamilyen egyszerű szó (főnév vagy cégnév) vagy jelszópróbálkozás (mint például "titok", ami meglepően egyszer sem szerepelt). Az első 100 leggyakoribb jelszó pedig mintegy 1100 felhasználói azonosítót fed le! [a vizsgált 7643-ból]".

A logikus (és helyes) megközelítés onnan indul, hogy egy jelszót akkor tarthatunk jónak, ha a felhasználó azt képes megjegyezni (nem fogja fölírni sehová), ugyanakkor viszont illetéktelenek nem tudják azt eredményesen megtippelni. Röviden: **legyen megjegyezhető és kitalálhatatlan.**

Vegyük szemügyre tehát a lehetséges kitalálási, megtippelési módszereket.

4.4.2 Kitalálási módok

A legkirívóbb eset az „alapértelmezett" jelsavak használata. Ez lehet gyári alapértelmezett beállítás (wifi-eszköz), amelyet a felhasználó nem változtat meg, vagy pedig a kényelmes ember ilyesféle jelszavai: asdfgh, 123456, password, jelszó, titok stb.

A következő csoportba azon esetek tartoznak, amikor logikai kapcsolat áll fenn a jelszó és a felhasználó személye, illetve a jelszó és a bejelentkezési név között. Az előbbire példa a születési dátum vagy a telefonszám jelszókénti használata, utóbbira példák: pistike – pistike12, pistike – pistike.pistike, pistike – ekitsip stb.

Ezen első két csoportba tartozó jelszó használata kimeríti a súlyos gondatlanság fogalmát. Aki ilyen jelszavakat használ, megérdemli a következményeket. Ha ezen módon nem vezettek eredményre, a következő lehetőség az ún. szótár alapú támadás alkalmazása.

A szótár alapú támadás esetén a támadó összegyűjti egy listába a leggyakoribb, legvalószínűbb jelszólehetőségeket és variánsokat, majd egy célprogram ezeket sorjában kipróbálja, találat esetén jelez. Ezen lehetőség arra indítja az elővigyázatos felhasználót, hogy olyan jelszavakat se alkalmazzon, amelyek bármilyen listában, szótárban, dokumentumban előfordulhatnak, illetve ezek kézenfekvő írásmódú változatait (pl. NemuannJanos).

A legvégső eset a nyers erő módszere (brute force). Ennek során egy célprogram az összes lehetséges jelszókombinációt kipróbálja. Nyilvánvaló, hogy ez a módszer mindenképpen megtalálja a helyes jelszót, az egyetlen fennmaradó kérdés csak az, hogy mennyi idő alatt. Tíz perc és tízezer év között nagy különbség van!

Számoljunk! Ha a jelszó hossza 8 karakter, és erősségét avval próbáljuk fokozni, hogy előírjuk: tartalmazzon kisbetűk mellett nagybetűket, számjegyeket és írásjeleket is, akkor a lehetséges kombinációk száma hatványfüggvény szerint

[9] Vajda et al., 2000.

növekszik (x^a), x az alap-karakterkészlet számossága, a a jelszóhossz). Az angol ábécé betűinek száma 26, van tíz számjegy, és mondjuk tízféle írásjel és speciális karakter: ez 26+26+10+10=72 karakteres alaphalmaz. A hat karakteres jelszavak száma kb. 140 milliárd (72^6). Ugyanez a lehetséges jelszószám elérhető csupán számjegyekből álló jelszó esetén is, ha annak hossza 12-13 számjegy. A jelszó hosszát növelve a lehetséges jelszavak számának növekedését nem hatvány-, hanem exponenciális függvény (a^x) írja le, az pedig gyorsabban növekszik, mint a hatványfüggvény. Ha figyelembe vesszük a megjegyezhetőség igényét is, adódik, hogy jobban járunk, ha a kitalálhatatlanság követelményét nem az értelmetlenség eszközével próbáljuk biztosítani, hanem inkább a hosszúsággal.

Számoljuk át a lehetséges darabszámokat megtalálási időigényre! Tegyük fel, hogy a próbálgatás sebessége 100.000 próba/másodperc. Ebben az esetben a fenti példában szereplő hat karakteres jelszó megtalálható a legrosszabb (legjobb;) esetben is kb. 16 nap és 3 óra alatt. Ha a jelszó nyolc karakteres, akkor ez az időigény már közel 230 esztendő, azonos próbálgatási kapacitással. Levonhatjuk azt a következtetést, hogy a 8 karakternél rövidebb jelszavak biztonsága kétséges.

Megjegyzendő, hogy a szótáron, illetve a nyers erőn alapuló próbálgatásnak akkor lehet egyáltalán esélye, ha sikerül a célrendszerből megszerezni valamilyen módon a kódolt jelszavakat tartalmazó állományt (árnyékjelszavak, shadow passwords). Normális esetben ugyanis, elemi biztonsági megfontolásból, nem tárolják magát a jelszót, hanem annak egy transzformáltját, amelyet a nyílt jelszóból kevés és gyors számítással elő lehet állítani, a transzformált jelszóból azonban a nyílt jelszót visszaszámolni reménytelenebb vállalkozás még a nyers erőn alapuló próbálgatásnál is.

Természetesen az utóbbi kétféle támadási mód hatékonysága jelentősen növelhető a próbálgatások sorrendjének optimalizálásával: ehhez azonban arra van szükség, hogy nagy mennyiségű, ténylegesen használt jelszó szerkezetének elemzésével általánosítható következtetéseket lehessen levonni az adott környezet és kor általános jelszóhasználati szokásairól.

4.4.3 Jelszógenerálási példák

A fenti körülmények figyelembe vételével egy lehetséges jelszóelőállítási mód egy, a felhasználó számára könnyen megjegyezhető (akár közismert) szövegelemnek a csak a számára logikus módon történő egyedi módosításán alapul. Legyen például a közismert szövegelem: „Talpra magyar”. Ennek egy lehetséges módosítása a „TalpraIIImagyar15?” (a felhasználó kissé szkeptikus). Az efféle módon előállított jelszó vélhetően ellenáll a szótár alapú támadásoknak is, mert az egyedi átalakításoknak olyan sok lehetséges, esetenként a *jelentéstől* is függő módja van, hogy azokat nem valószínű algoritmikusan sikeresen leírni. Figyelem: a közismert karaktercserék (1 számjegy és l betű stb.) nem jó ötlet, éppen közismert és általánosan elterjedt mivoltuk miatt. A példabeli jelszó 19 karakter hosszúságú, nyers erővel történő megtalálása a fentebb feltételezett

sebességgel is olyan sok évet venne igénybe, amelynek kimondására nincs szava a nyelvünknek (~10^{24} év, lényegesen több, mint világegyetemünk jelenlegi formájában életkora).

4.4.4 Kerülő utak

A jelszó minősége, jósága alapvető elővigyázatossági és biztonsági követelmény. Nem sokat ér azonban, ha a jelszó megszerzésének eszközei a sikeres tippelés helyett más síkra tevődnek át. A jelszó minősége teljesen közömbös, ha egy álmennyezetbe rejtett apró kamera, vagy egy hardveres billentyűzetnaplózó[10] rögzíti azt, vagy pedig adathalász becsapásnak (phishing) bedől a felhasználó.

5 Illetéktelen hozzáférés ellen

Illetéktelen az, akit az adat birtokosa annak vél – a továbbiakban pusztán technikai kérdésként kezeljük. Ebben a vonatkozásban a magánadatok és a céges adatok egyformák. A probléma korunkban fokozottan van jelen, ugyanis a digitálisan tárolt adatok illetéktelen eltulajdonítására jóval több lehetőség van, mint korábban a hagyományosan – papíralapon – tárolt adatok esetében. Az ipari kémkedés, lehallgatás, adatmegszerzés külön iparággá vált, és persze az ellene való védekezés is. Nyilvánvalóan nem lehetséges itt a témakört a maga teljességében feldolgozni, csak néhány alapvető fontosságú elemére térünk ki.

Általános szabályként, mint nyilvánvalót jelentjük ki, hogy a védelem és az éberség (l. ott) ezen a területen is kulcsfontosságú. Külön kiemelendő, hogy az adatainkhoz, illetve általánosabban mondva az erőforrásainkhoz való illetéktelen hozzáférés növeli az adatvesztés kockázatát is.

Adataink megvédése az illetéktelen hozzáféréstől mindig kétszemélyes, nullától különböző összegű játék, azaz a védő mindig többet veszít, mint amennyit a támadó (sikere esetén) nyer.

5.1 Titkosítás

Annak megnehezítésére, jobb esetben lehetetlenné tételére, hogy adatainkhoz illetéktelenek hozzáférjenek, az egyik legkézenfekvőbb mód azok titkosítása. A titkosítás történetének túlnyomó része a kommunikáció titkosításából áll, ugyanis a tárolt adatok titkosítása a számítógépes háttértárak kapcsán került előtérbe. A számítástechnika fejlődésével párhuzamosan a titkosítástan (a kriptográfia) külön

[10] Hardware keylogger, a billentyűleütések rögzítésére szolgáló apró eszköz, a számítógép és a billentyűzet közé kell elhelyezni, mintha egy apró hosszabbító lenne. Szoftveres úton nem kimutatható, típustól függően képes lehet mondjuk félmillió billentyűleütést rögzíteni, ára hozzávetőleg 100 USD.

tudományággá vált, a hagyományos, papír alapú és a mechanika törvényeire épülő világ számos, alapvető fontosságú megoldásának teremtette meg a digitális megfelelőjét, a digitális aláírástól kezdve az időbélyegzésen keresztül az olyan problémák megoldásáig, hogy egy adott titkosított dokumentumot csak adott öt ember közül három – és bármelyik három – együttesen tudjon csak dekódolni.

A területnek igen bőséges szakirodalma van, ezek egy része mélyebb matematikai ismeretek nélkül is haszonnal forgatható.[11]

5.2 Egykulcsos titkosítás

Az egykulcsos (szimmetrikus) titkosítás esetén ugyanazt a kulcsot használják a titkosításhoz és a fejtéshez. A titkosítás történetének túlnyomó része ilyen megoldások kifejlesztéséből (és elvérzéséből) áll. Verne Gyula: 800 mérföld az Amazonason c. regényének központi eleme egy titkosírás és annak az utolsó pillanatban sikeres megfejtése. A megfejtést a regényben az teszi lehetővé, hogy a Vernam-módszert ekkor még nem ismerték – és persze a „happy end" szüksége.

Az első világháború idején fejlesztette ki Gilbert Vernam azt a módszert – a Verne regényben használt módszer általánosítása –, amelynek elvi megfejthetetlenségét később Shannon bizonyította be.

5.2.1 Elvi megoldás

Feltehetően mindenki ismeri, vagy legalábbis el tudja képzelni azt a módszert, amikor két ember megállapodik egy számban (ez a kulcs), és abban a módszerben, hogy az üzenet minden egyes betűjét a megállapodott számnak megfelelő hellyel tolják el az ábécében. Nyilvánvaló lehet bárki számára, hogy egy ilyen eljárás igen könnyen megfejthető a „kulcs" ismerete nélkül is, egyszerű statisztikai vizsgálattal (betűgyakoriság). Az is nyilvánvaló lehet, hogy ha nem egyjegyű, hanem kétjegyű, háromjegyű stb. számot használnak, ez a megfejtés valamivel nehezebbé válik, hiszen a titkosított szövegben a leggyakoribb betűknek nem mindig ugyanaz, hanem két, három stb. más betű fog megfelelni. Azt is sejthetjük mélyebb matematikai bizonyítás nélkül, hogy a kulcs hosszának növelésével az illetéktelen (a kulcs ismerete nélküli) megfejtés egyre nehezebbé válik ugyan, egyre több titkosított szövegre van hozzá szükség, de nem lesz elvileg lehetetlen.

Ha azonban a kulcs egy valódi véletlen számsorozat, akkor a kulcs ismerete nélküli megfejtés lehetetlenné válik, hiszen a kulcs valódi véletlen sorozat mivolta miatt nincs statisztikailag megfogható szabályszerűség (sem semmilyen más), ami támpontot adhatna a fejtéshez. Nem csoda, ez a titkosítási eljárás A+B=C alakban írható fel általánosan, ahol A a nyílt szöveg, B a kulcs és C a titkosított szöveg. Ha

[11] L. pl. Nemetz, 1995., Ködmön, 2002.

C lehallgatható a valahol megbízhatatlan interneten, de B-re nézve semmilyen támpont nincs, akkor nem lehet szűkíteni a kört: tetszőleges nyílt szöveghez létezik olyan kulcs, amelynek alkalmazása C-t eredményezi (vagy tetszőleges kulcshoz létezik olyan nyílt szöveg, amelynek titkosított párja pont C).

Az összeadás itt nem feltétlenül matematikai értelemben vett összeadást jelent, bármilyen művelet alkalmazható, ha az bájtonként elvégezhető, és van inverze (pl. XOR). Vegyünk egy konkrét példát. Írjuk le a titkosítandó szöveget, alája a kulcs számsorozatát, majd minden betű helyett vegyük az ábécében* annyiadik rákövetkezőt, amilyen számjegy alatta áll, ha a végére érünk, természetesen kezdjük elölről:

```
EZ ITT A NYÍLT SZÖVEG, ALATTA A KULCS, AZ ALATT A
TITKOSÍTOTT SZÖVEG
92689070027803779226817274578488646654656436704626318045403341106861
L,ÓÓZTAA
Ó:ÖLÜAWÁPXÍN.ABPDVXG?GÁÖVŐHŰ:ÓE:?CŐFTŰÓBÓÜÍYKPŰMTŐÜŰ
,TZT!ÍH
```

* A példában alkalmazott ábécé:
AÁBCDEÉFGHIÍJKLMNOÓÖŐPQRSTUÚÜŰVWXYZ<szóköz>,.!?:

A módszer két alapvető biztonsági szabálya: a kulcsnak valódi véletlen sorozatnak kell lennie, és garantáltan titokban kell maradnia, azaz csak a kommunikáló felek ismerhetik azt. A valódi véletlen sorozat mivolt azt is jelenti, hogy nem szabad egynél többször felhasználni azt. A garantált titokban maradás követelményének egyik következménye, hogy a kulcs cseréjéhez biztonságos csatorna szükséges (pl. személyes találkozás), ami esetenként nehézkessé, illetve drágává teszi azt. Evvel együtt is megvan a létjogosultsága: például a diplomáciában (a nagykövet időnként mindenképpen hazautazik, viheti magával az új kulcsot a következő időszakra). Gyakorlati nehézség, hogy valódi véletlen sorozatokat nem könnyű előállítani.

5.2.2 Gyakorlati megoldás

A valódi véletlen sorozatok előállítási és kezelési nehézségei miatt a fenti, ún. folyamkódolás helyett a gyakorlatban ún. blokk-kódolási eljárásokat alkalmaznak. Ennek során a nyílt szöveget kisebb blokkokra bontják és azokat kódolják valamivel bonyolultabb eljárásokkal. A DES (Data Encryption Standard) 1976-ban vált szabvánnyá, amely 64 bites blokkokat titkosított 56 bites kulccsal. A számítási teljesítmények javulásával azonban ez az eljárás a kicsiny kulcsméret miatt jó ideje nem számít kellően megbízhatónak. Számos más, biztonságosabb (vagy annak tartott;) blokk-kódoló eljárás létezik (3DES, AES stb.).

5.2.3 Előny-hátrány

Az egykulcsos eljárás vitathatatlan előnye, hogy nem igényel jelentős számítási teljesítményt, folyamkódolás esetén akár elvileg megfejthetetlen is lehet, míg a blokktitkosító eljárások fejtésére léteznek különféle módszerek, amelyek különféle feltételek teljesülése esetén akár eredményesek is lehetnek.

Probléma viszont a kulcs cseréje, amelyhez biztonságos csatornára van szükség, ami akár igen körülményes vagy drága is lehet.

Természetesen nem lehet eltekinteni attól a kézenfekvő lehetőségtől, hogy a titkosított üzenet tartalmát formális megfejtés helyett valamilyen kerülő úton, például elektronikus lehallgatással szerezze meg az ebben érdekelt fél. Ennek lehetősége és esetleges eredménye azonban független a módszer matematikai értelemben vett jóságától.

5.2.4 Titkosított lemezegységek

A tárolt adatok titkosítására az egyes fájlok titkosítása nem a legmegfelelőbb eljárás. Nemcsak nehézkessége és az emberi hibatényező miatt, hanem azért is, mert a legnagyobb felhasználói gondosság mellett is megmaradhat a védendő fájlok egy része, esetleg egésze nyílt állapotában (ideiglenes fájlok, lapozómemória stb.). Ezért a teljes partíció vagy a teljes lemezegység titkosítása jobb ötlet.

A teljes partíció (lemezegység) kódolása-dekódolása valós időben történik, a szektor szintű lemezírási, -olvasási műveletek során, és a mai gépeken nem okoz számottevő teljesítménycsökkenést. A titkosításhoz, illetve a dekódoláshoz használt kulcs a felhasználó által választott jelszó alapján készül, a jelszó nélkül az eredeti adattartalom nem állítható elő. Ha tehát elég jó jelszót választ a felhasználó (l. a Jó jelszó c. részt), a szótáron vagy a nyers erőn alapuló feltörés reménytelen.

Lehetőség van a titkosított lemezegységek egymásba ágyazására is, ez esetben a beágyazott lemezegység nemcsak titkos, de jó esetben a puszta létezése sem megállapítható.

Fontos szempont, hogy ilyen célra lehetőleg szabad szoftvert használjunk. Ez esetben ugyanis a forráskód szabad hozzáférhetősége és ellenőrizhetősége miatt igen kicsi az esélye annak, hogy abban valamilyen „hátsó kapu” legyen elrejtve. Zárt, üzleti szoftver esetében ilyen biztosíték nincs, el kell hinnünk a termék fejlesztőjének, hogy tényleg nem épített be ilyent a programjába.

5.3 Kétkulcsos titkosítás

Az egykulcsos titkosításnak a kulcscserével kapcsolatos nehézségeit szünteti meg a kétkulcsos titkosítás: itt nem szükséges biztonságos csatorna a kulcs cseréjéhez. Rivest, Shamir és Adleman 1976-ban publikálták a neveik kezdőbetűiről

elnevezett RSA-algoritmust, amely kiküszöböli a kulcscsere problémáját. Ennek azonban ára van: a titkosítás megfejthető a megfelelő kulcs nélkül is – elméletileg, azaz ismert a fejtés algoritmusa, de ez belátható idő alatt nem végezhető el a valóságban. Az eljárás alapja az, hogy a matematikában vannak olyan műveletek, amelyeket aránylag könnyen és gyorsan el lehet végezni, míg az inverz művelet reménytelen. Például két „nagy" prímszámot összeszorozni még papíron is lehet (ha nagyon muszáj), ellenben a szorzat prímfelbontását az eredeti tényezők ismerete nélkül megcsinálni erősen reménytelen, olyan nagy mennyiségű osztást kellene elvégezni.

5.3.1 Elvi megoldás

A rendszerben résztvevő feleknek két – összetartozó – kulcsuk van: egyiket titkosnak kulcsnak nevezzük, és a felet titokban tartják, csak a tulajdonosa ismerheti azt. A másik kulcsot nyilvános kulcsnak nevezzük, és gazdája bárkivel közölheti, sőt kimondottan előnyös, ha minél többen ismerik azt.

Az RSA-eljárás alapelve, hogy ha az összetartozó kulcspár egyik felével kódolunk valamit, az csak és kizárólag annak párjával dekódolható. A titkos kulcsot T-vel, a nyilvánosan N-nel jelölve, formálisan:

`kódolás[kódolás(szöveg,N),P]=szöveg`

illetve

`kódolás[kódolás(szöveg,P),N]=szöveg`

A fenti meghatározások alapján tehát ha Aladár titkosított üzenetet akar küldeni Beának, Bea nyilvános kulcsára (N_B) van szüksége, amelyet – lévén a kulcs nyilvános, bárki számára hozzáférhető – megszerezhet, birtokolhat. Az ezen kulccsal titkosított üzenetet annak titkos párjával (T_B) lehet dekódolni, márpedig Bea titkos kulcsa a definíció értelmében csak és kizárólag Bea birtokában lehet, azaz a titkosított üzenetet hiába szerzi meg bárki is pl. a hálózati adatforgalom lehallgatásával, Bea titkos kulcsa híján azt képtelen lesz belátható időn alatt megfejteni.

Bea számára természetesen kérdéses, hogy a titkosított üzenet valóban Aladártól származik-e. Ha például Aladár a saját titkos kulcsával (T_A) titkosítja az üzenetet, azt ugyan nemcsak Bea, de bárki is képes dekódolni, hiszen ehhez a művelethez Aladár nyilvános kulcsára van szükség. Ha a dekódolás sikeres, akkor a feladó valóban Aladár (hiszen T_A kizárólag Aladár birtokában lehet, és ha az üzenetet N_A-val lehet dekódolni, akkor azt T_A-val kódolták. Ezen lépés azonban a tartalom hitelességéről nem mond semmit, az üzenet útközben akár meg is változhatott – mondjuk véletlen adatátviteli hiba következtében;) A digitális aláírás ezen lépés módosított változata, l. ott.

A módszer két alapvető fontosságú biztonsági szabálya, hogy a titkos kulcsát minden érdekelt fél biztonságosan tárolja és őrzi, az semmilyen körülmények

között nem kerülhet más birtokába (az ugyanis nemcsak azt jelenti, hogy a megszerzett titkos kulcs birtokában könnyen fejthető a kulcs gazdájának címzett titkos üzenet, de annak birtokában a jogos gazdája nevében digitális aláírást is lehet készíteni). A másik fontos szabály, hogy az összegyűjtött nyilvános kulcsok hitelességéről azok használata előtt meg kell győződni, ennek híján fennáll a közbeékelődéses támadás lehetősége (l. ott).

Hogyan lehet meggyőződni egy begyűjtött nyilvános kulcs hitelességéről, arról, hogy a kulcs valóban azé a személyé, akiének látszik, akiének hisszük? Erre számos lehetőség van. A legkézenfekvőbb és legbiztosabb, ha a nyilvános kulcsot személyesen a gazdájától kaptuk. Ha azonban erre nincsen mód – és általában nincsen, pont emiatt találták ki a kétkulcsos titkosítást –, más lehetőségeket kell keressünk. Ha jól ismerjük a másik felet, megoldás lehet az emilben kapott nyilvános kulcsot telefonon ellenőrizni. Elküldhetjük a kulcsot emilben, hagyományos postán, távmásolón és SMS-ben is. Ha mindegyik csatornán ugyanaz a kulcs érkezik meg a címzetthez, igen kicsi a valószínűsége annak, hogy azt útközben manipulálhatta valaki, gyakorlatilag csak gondosan tervezett titkosszolgálati akció keretében képzelhető el. Ezeken kívül, általános esetben a megoldást a digitális aláírás alkalmazásával kiépülő bizalmi háló adja (l. Tanúsítványok).

5.3.2 Előny-hátrány

A módszer vitathatatlan előnye, hogy nem szükséges a kulcsok cseréjéhez biztonságos csatorna, a nyilvános kulcsokat ugyanis bárki ismerheti, így azokat akár emilben is el lehet küldeni, bár a kapott nyilvános kulcsok hitelességéről – valóban ahhoz a személyhez tartozik, akiének véljük – igencsak célszerű meggyőződni.

Hátránya a módszernek, hogy elvileg megfejthető a titkos kulcs ismerete nélkül is, „csak” gyakorlatilag lehetetlen.

5.3.3 Digitális aláírás

A digitális aláírásnak a hagyományos aláírással megegyező módon az aláíró személyén kívül azt kell bizonyítania, hogy az aláírt dokumentum tartalma az aláírás után nem változott meg. A hagyományos aláírás ezt a dokumentum hordozóanyagának (papír, esetleg pergamen) egyértelműen személyhez kötődő megjelölésével (kézi aláírás) biztosítja, mivel a hétköznapi életben nincs lehetőség egy dokumentumnak az aláírást tartalmazó alját levágni és nyomok nélkül egy másik papírhoz csatlakoztatni.

A digitális aláírás esetében mindezt matematikai úton kell megvalósítani. A fentebbi gondolatmenetet csak kicsit kell módosítani ahhoz, ne csak a feladó személye, hanem a tartalom változatlansága is bizonyítható legyen.

Első lépésben az aláíró kiszámol egy fix hosszúságú ellenőrző összeget (S_0) az

aláírandó dokumentumból egy matematikai eljárással (hash v. hasító függvények). Ezt az ellenőrző összeget titkosítja az aláíró saját titkos kulcsával, majd ennek eredményét mellékeli a dokumentumhoz, pl.:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Ez itt egy teszt emil a digitális aláírás
bemutatására. Ez maga az
aláírt szöveg. Írta és aláírta: Keszthelyi András
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: Using GnuPG with Mozilla -
http://enigmail.mozdev.org/

iQEcBAEBAgAGBQJPoZcWAAoJEPQFQQClpiDS5fIH/2MBWdy+ap7j
ayb+sSJrJlYt
F5LsJ3jPZR0GzdODmUSkmsiD3w299yxTES6L7ZaO1l79j6/oKHnN
4erpOMv3urjN
1tWAccLBWDsNPreUOpFSNnShBndrhL6+zrzYKZ2oMhuTh2Yy0fmP
LsN0z/7Ka3dq
QYfxMwLGuVEH+NMbCk89BxH+wGAmc6nyrAgUjQU+c+w+zxhD17Au
0rC5uB+tB7lp
6ovf6dxA5pgbNZOWUPrL3am5/mp5uC54Pk7+bbHPHc1e+KMywJWR
jpibRRu8DA+j
q6i5+KHXunVaaFlzHDE/j8YyINOs0wlNEgtBS/GUnLMNxHz0TEHH
Zhh3NBCQtpU=
=AT1o
-----END PGP SIGNATURE-----
```

A címzett az aláírást úgy ellenőrzi, hogy első lépésben ő is kiszámolja a dokumentum ellenőrző összegét ugyanavval az eljárással (példánkban SHA1), mint az aláíró. Legyen ez S_1. Majd dekódolja a feladó által titkosított ellenőrző összeget a – vélt – feladó nyilvános kulcsával, legyen ennek eredménye S_2. Ha $S_1=S_2$, akkor mind a feladó, mind a tartalom hiteles. Ha ugyanis a feladó hiteles, akkor $S_0=S_2$, míg a tartalom változatlanságát az $S_0=S_1$ fennállása bizonyítja. Ugyan az eredeti S_0-t bizonyítottan nem ismerjük, de a két összefüggésből annak értékétől függetlenül, általánosan következik, hogy $S_1=S_2$ kell teljesüljön, ha minden rendben van.

A digitális aláírást tekinthetjük úgy is, mint egy kétváltozós függvényt. Az egyik bemenő adat az aláírandó dokumentum, legyen ez bármilyen bájtsorozat, a másik bemenő adat pedig az aláíró titkos kulcsa. A függvény ezen két adatból számítja ki matematikailag azt az eredményt, ami maga a digitális aláírás. A függvénynek nincs inverze, az aláírásból sem az eredeti dokumentum tartalma, sem az aláíráshoz használt titkos kulcs nem számolható ki.

Vigyázat! A hagyományos aláírás bioemetrikus azonosító, és vita esetén írásszakértők bizonyíthatják annak eredetiségét vagy hamis mivoltát. A digitális aláírás viszont nem biometrikus, hanem birtoklás alapú azonosítást jelent: akinek birtokában van az adott titkos kulcs, az készíthet digitális aláírást. Nincs lehetőség az aláírás hamisságának írásszakértői vizsgálatára.

5.3.4 Tanúsítványok

Mivel bármilyen dokumentumot, általánosabban fogalmazva bármilyen bájtsorozatot alá lehet írni digitálisan, nyilvános kulcsokat is el lehet látni digitális aláírással. Pontosabban nem csupán magát a nyilvános kulcsot, hanem egy olyan dokumentumot, amely tartalmazza a személy (vagy cég) nevét és a nyilvános kulcsát. Ha kapok emilben egy nyilvános kulcsot, nem lehetek bizonyos benne, hogy az valóban azé, aki a feladónak látszik. Ha azonban kapok egy olyan dokumentumot, amely egy nyilvános kulcsot és gazdájának fontosabb adatait tartalmazza, és ezt egy olyan valaki írta alá digitálisan, akinek a nyilvános kulcsát korábban már valahogy ellenőriztem, és hitelesnek találtam, akkor biztos lehetek benne, hogy a most kapott nyilvános kulcs valóban a jelzett személyé.

Tegyük fel például, hogy Aladár régebbről birtokolja Bea nyilvános kulcsát, és mivel azt még személyesen kapta Beától, abszolút hitelesnek tekinti. Később Cecília megkéri Beát, hogy írja alá Cecília nyilvános kulcsát. Bea tehát készít egy dokumentumot, amely kb. azt tartalmazza, hogy „Az alábbi nyilvános kulcs Cecíliáé, <nyilvános kulcs>”, majd digitálisan aláírja azt. Ezt az aláírt dokumentumot Cecília elküldi Aladárnak (bárkinek, aki Bea aláírását ellenőrizni tudja). Aladár, Bea hiteles nyilvános kulcsának birtokában ellenőrizni tudja az aláírást, és elfogadhatja Cecília nyilvános kulcsát is hitelesnek, mert Aladár személyesen meggyőződött arról, hogy az adott személy és az adott nyilvános kulcs összetartoznak. A későbbiekben pl. Cecília hasonlóképpen aláírhatja Dezső nyilvános kulcsát – tanúsítja, hogy a nyilvános kulcs és Dezső összetartoznak –, és ezt Aladár azért fogadhatja el, mert Cecília nyilvános kulcsát elfogadta hitelesnek, mert azt Bea saját aláírásával hitelesítette, más szóval tanúsította. Akár egy hagyományos dokumentum esetében a hagyományos tanúk. Így épül a bizalmi lánc.

Nyilván egy dokumentumot akárhány személy is aláírhat, digitálisan is, tehát semmi akadálya nincs annak, hogy bárki aláírja digitálisan bárkinek a nyilvános kulcsát – természetesen, miután meggyőződött arról, hogy az adott személy valóban az, akinek mondja saját magát –, így az egyes nyilvános kulcsokon több digitális aláírás is lehetséges; nemcsak bizalmi láncok alakulhatnak, hanem – jobb esetben – bizalmi háló is. Vegyük észre, hogy ehhez semmilyen központi szerv, szereplő nem szükséges!

Ha ezt az aláírási folyamatot intézményesítjük, a tanúsítványszolgáltató fogalmához jutunk. Egyes vállalkozások anyagi ellenszolgáltatás fejében aláírják a fentebb bemutatott dokumentumot, pontosabban annak szabványosított

változatát[12], miután az elvárható módon meggyőződtek arról, hogy az aláírást kérő személy valóban az, akinek kiadja saját magát. Természetesen egy ilyen vállalkozás csak akkor lesz működőképes, ha biztosítani tudja valami módon, hogy az ő nyilvános kulcsának hiteles példánya könnyen megtalálható és elérhető legyen szerte a világban, hogy az általa kibocsátott tanúsítványokat ellenőrizni lehessen.

A magyarországi formális jog szabályozás vonatkozásában l. a 2001. évi XXXV. törvényt az elektronikus aláírásról, ide értve azon feltételek meghatározását, amelyek teljesülése esetén a digitális aláírás a hagyományos aláírással egyenértékű jogi szempontból is.

5.4 Alkalmazások és problémák

5.4.1 Biztonságos böngészés (https)

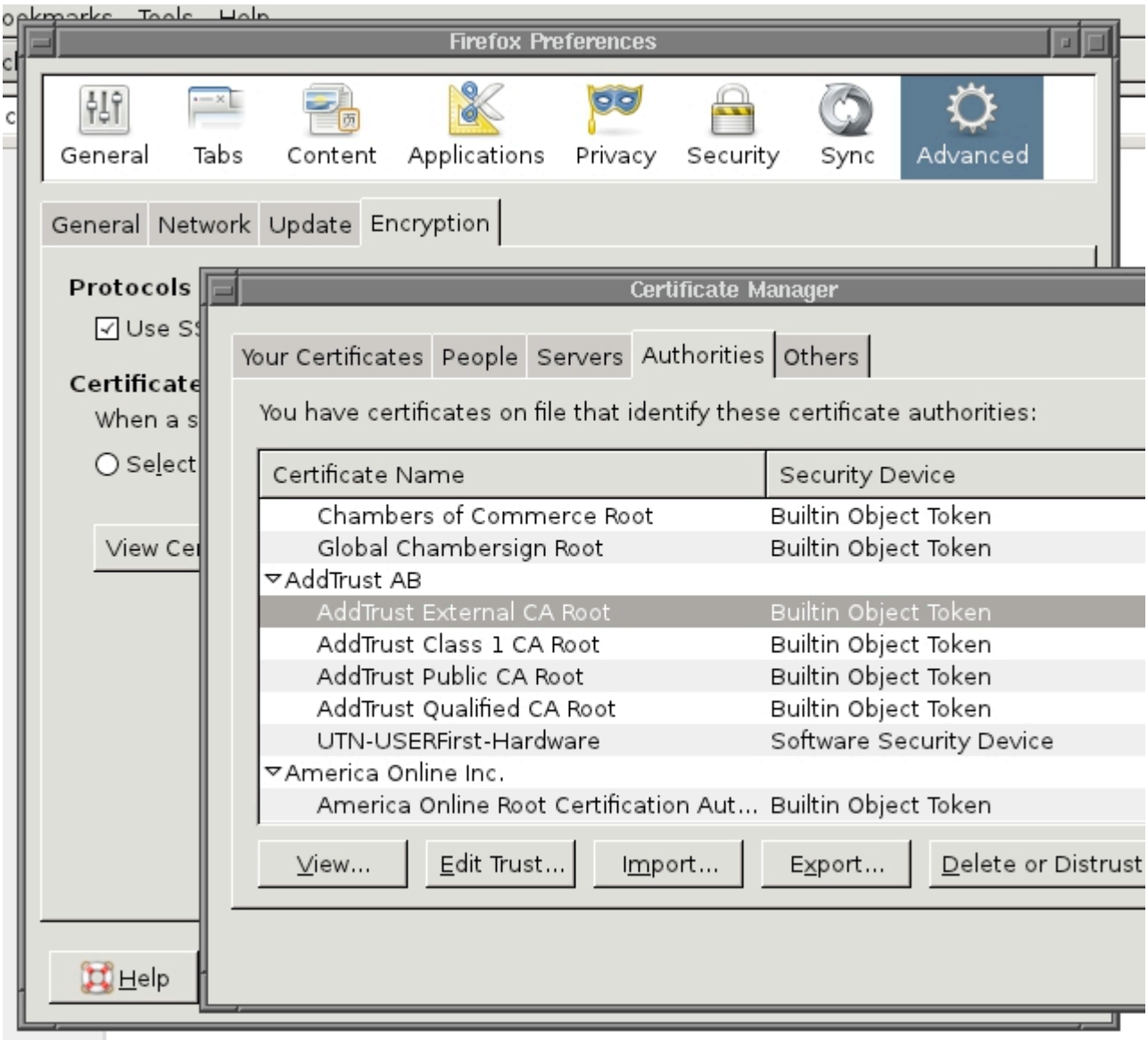
A hagyományos adatátviteli módok (prtokollok) mind nyílt szöveg alapúak, azaz a teljes adattartalom, ide értve a felhasználói neveket és jelszavakat is, nyílt szöveg formájában halad végig a hálózaton. Ez azt jelenti, hogy ezen adatok igen könnyen lehallgathatóak. Korunkban így nem lehetne érzékeny adatokat tartalmazó kommunikációt megvalósítani, pl. interneten vásárolni, bankolni stb. Fölmerül tehát, illetve fölmerült az igény arra, hogy ezt az eredetileg nyílt adatátvitelt biztonságossá, pontosabban titkossá lehessen tenni. Böngészés esetében erre való a https (Hypertext Transfer Protocol over Secure Socket Layer) protokoll.

Figyelembe véve korunk – jogos – igényeit, az eljárás a kétkulcsos titkosítást használja. Mi történik tehát, ha a böngészőbe pl. a https://neptun.uni-obuda.hu címet írjuk be? A böngésző megkapja a kiszolgáló tanúsítványát, benne annak nyilvános kulcsát, és megpróbálja ellenőrizni azt. Esetünkben a tanúsítványt a Terena SSL CA bocsátotta ki, és 2012. február 27-től számítva három évig érvényes. A Terena SSL CA tanúsítványát az UTN-USERFirst-Hardware bocsátotta ki (érvényes 2005. június 7-től 2020. május 30-ig). Ez utóbbinak a tanúsítványát az AddTrust External CA Root nevű cég bocsátotta ki (érv. 2000. május 30-tól 2020. május 30-ig). Az AddTrust tanúsítványát *saját maga* bocsátotta ki.

Ez azt jelenti, hogy a bizalmi lánc nem követhető tovább, a tanúsítvány mégis ellenőrizhető. A böngészők ugyanis jó néhány nagy, nemzetközi tanúsítványkibocsátó cég (CA) saját tanúsítványát „gyárilag” tartalmazzák – így az AddTrust tanúsítványát is –, ami megfelel annak az esetnek, ha valakinek a nyilvános kulcsát személyesen a gazdájától kapjuk meg. Ez esetben tehát a böngésző elfogadja megbízhatónak a Neptun-kiszolgáló tanúsítványát, benne annak nyilvános kulcsát, mivel annak hitelességét vissza lehetett vezetni egy

[12] L. pl. RFC 2459, Internet X.509 Public Key Infrastructure, http://www.ietf.org/rfc/rfc2459

hiteles, legfelső szintű tanúsítványra.

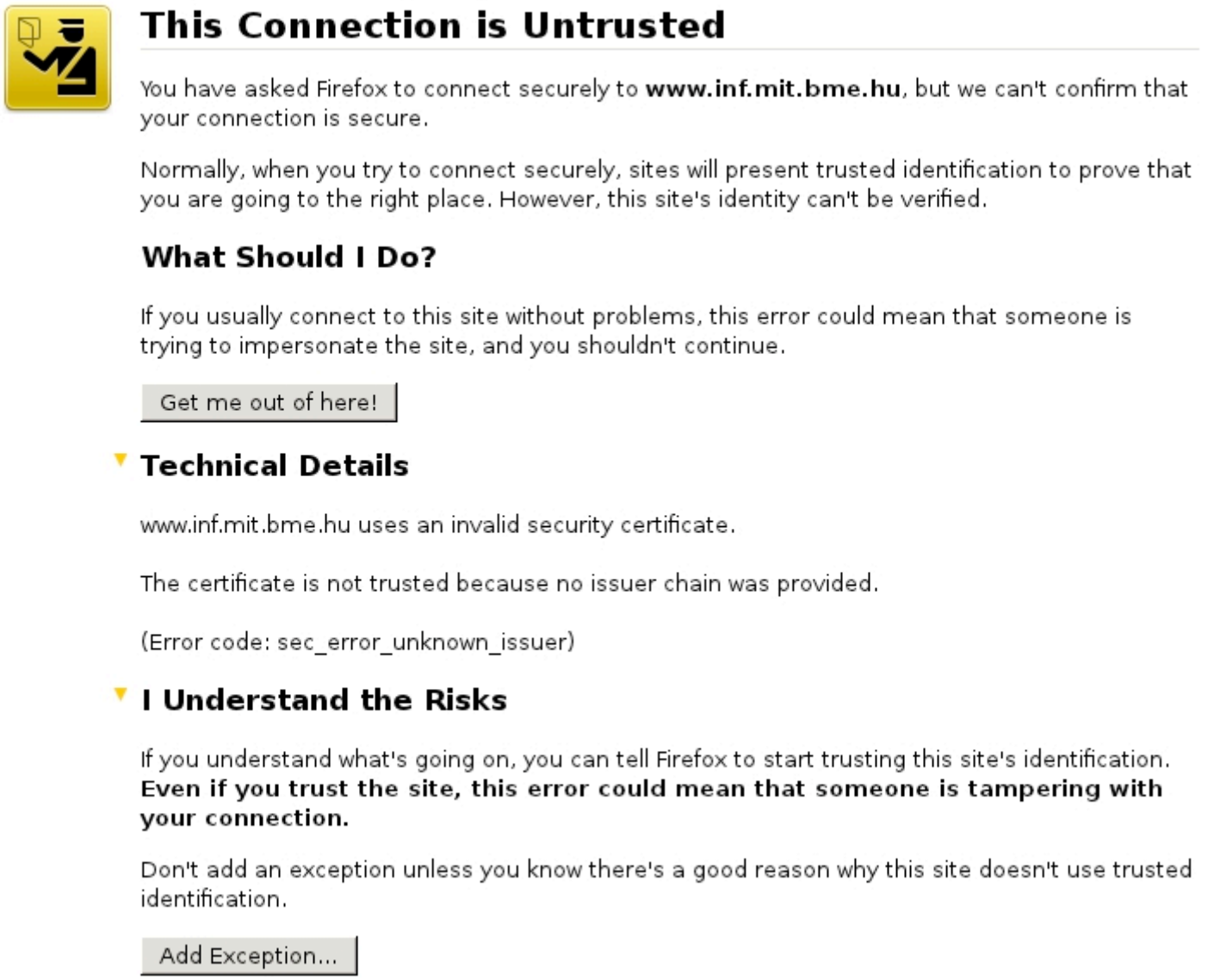


1. ábra

A böngészőbe (Firefox 4.0) gyárilag beépített tanúsítványok listája

Ha a tanúsítványok láncát a böngésző nem tudja visszavezetni egyik általa tárolt, legfelső szintű tanúsítványra sem, akkor hibaüzenetet ad. Ilyen esetben nem célszerű folytatni – pontosabban elkezdeni – a műveletet, amíg meg nem

győződünk róla, hogy az elérni kívánt kiszolgáló tanúsítványát azért nem lehet ellenőrizni, mert – technikai okok miatt – nem tudja a böngésző visszavezetni a tárolt tanúsítványok egyikére sem, vagy pedig mert éppen közbeékelődéses támadást próbál valaki megvalósítani. Ez az egyedi, „kézi" ellenőrzés esete, példánkban az egyetem informatikai osztályán (telefonon) egyeztethetnénk a Neptun-kiszolgáló tanúsítványát. Ha ez sikeres (azaz kizártuk a közbeékelődés lehetőségét), nyugodt lelkiismerettel kattinthatunk a böngésző „megértettem a kockázatot, folytassuk a műveletet" jelentéstartalmú gombjára.



2. ábra
Firefox 4.0 böngésző hibaüzenete sikertelen tanúsítványellenőrzés kapcsán

5.4.2 SSH: kaputovábbítás

Az SSH (Secure Shell) távoli számítógépre való biztonságos bejelentkezést tesz lehetővé (titkosított csatornán keresztül). Ezen túl képes kaputovábbításra (port forwarding) is, amelynek segítségével a hagyományos, nem titkosított adatátviteli

protokollokat tudjuk az SSH által titkosított csatornába (ssh-alagút) terelni és így biztonságossá tenni. Alkalmazási példák: l. Vállalkozásfejlesztés a XXI. században, szerk. dr. Nagy Imre Zoltán, ÓE, Bp. 2011., pp. 99-109.

5.4.3 MITM

Ha egy ellenőrizetlen nyilvános kulcsot használunk az elküldendő üzenet titkosítására, fennáll a lehetősége a közbeékelődéses támadásnak (man-in-the-middle attack). Ez úgy történhet meg, ha egy személy (területileg illetékes rendszergazda pl., nevezzük Cillának) technikailag képes szűrni az átmenő emilforgalmat. Tegyük fel, hogy Aladár szeretne titkosított üzenetet küldeni Beának. Elkéri Bea nyilvános kulcsát, amit Bea emilben elküld Aladárnak. Ezt az emilt eltérítve a mellékelt nyilvános kulcsot Cilla kicserélheti a sajátjára, majd továbbküldi az emilt. Aladár ekkor tehát megkapja Cilla N_C nyilvános kulcsát, de azt hiszi, hogy az Bea N_B nyilvános kulcsa. Ha Aladár a kapott nyilvános kulcsot ellenőrzés nélkül felhasználja, akkor megvalósulhat a sikeres támadás. Az Aladár által N_B-vel titkosított üzenetet Cilla megint csak eltéríti, a birtokában lévő T_C-vel dekódolja, szükség esetén megváltoztatja a tartalmát, majd az általa félretett, igazi N_B-vel újra titkosítja és továbbküldi Beának. Bea pedig azt hiszi, hogy az üzenet Aladártól származik, és hogy senki más nem ismeri annak tartalmát.

A https böngészés esetén is megvalósítható lehet a közbeékelődés, például ha sikerül valami módon a felhasználó gépén manipulálni a böngésző által tárolt tanúsítványokat (és becsempészni közéjük egy hamis legfelső szintűt, vagy a megcélzott rendszer hamis tanúsítványát a felhasználó által ellenőrzöttek közé), vagy akkor, ha a célrendszer tanúsítványa adott időszakban nem ellenőrizhető automatikusan, tehát a felhasználók hozzászoktak az erre vonatkozó figyelmeztető ablakhoz, és – eléggé el nem ítélhetően – ahhoz, hogy azt vizsgálódás nélkül „leokézzák”.

5.4.4 Levelezés: Thunderbird és Enigmail

Az elektronikus levelezésről a legtöbb embernek manapság a webes felületen, böngészővel elérhető ingyenes levelezők (gmail.com, freemail.hu, citromail.hu, vipmail.hu stb.) jutnak az eszébe. Az elektronikus levelezés hagyományos módon azonban nem így történik, hanem valamilyen levelezőprogram használatával. Egy levelezőprogram használata számos előnyt biztosít a webes felületű levelezéshez képest: a levelek kezelésével kapcsolatos műveletek kényelmesebb, hatékonyabb végzésén túl a leveleknek a felhasználó gépére való letöltődése vitathatatlan előny, nemcsak az offline használat lehetősége miatt, hanem adatmentési szempontból is. Idők folyamán rengeteg különféle levelezőprogram készült és létezik ma is. A legismertebbek a Kitekintő Gyorsvonat (Outlook Express) és a Mennydörgő Madár (Thunderbird).

A hagyományos levelezés két protokollt használ: küldéshez az SMTP-t (Simple Mail Transfer Protocol, 25-ös port), fogadáshoz a POP3 (Post Office Protocol 3,

110-es port) vagy az IMAP (Internet Message Access Protocol, 143-as port). A hagyományos levelezéshez kliensprogramot használunk (mert kényelmesek vagyunk;), ilyen pl. a Thunderbird, de van számos más is. A hagyományos levelezés során az emilek letöltődnek a kliens gépre, POP3 esetén mindközönségesen, IMAP esetén a kliens gépen végzett rendezgetés, mappákba sorolás visszaszinkronizálható a kiszolgálóra, így levelezésünk két, egymástól távol eső helyen található meg, összehangolt állapotban – vö. biztonsági mentés. Az, hogy az IMAP használata mellett webes felületen (webmail) is elérhetők-e leveleink (vagy fordítva), az kizárólag attól függ, hogy a kiszolgáló üzemeltetője telepített-e ilyen szolgáltatást. Az ingyenes szolgáltatók jó része is biztosít IMAP/SMTP elérést is a webmail mellett.

A Thunderbird levelezőprogramhoz tartozik egy Enigmail[13] kiegészítő, amely az elektronikus levelezésben kényelmesen használhatóvá teszi a kétkulcsos titkosítást, és ennek részeként a digitális aláírást.

5.4.5 Kerülő utak

Mivel a kétkulcsos titkosítás elméletileg ugyan megfejthető, de ennek gyakorlati kivitelezése több mint nehézkes, nem szabad figyelmen kívül hagynunk annak lehetőségét, hogy megfejtés helyett valamilyen kerülő úton próbálják megszerezni tőlünk a kívánt adatokat. Ezen kerülő utak a lehető legváltozatosabbak lehetnek, a teljesség igénye nélkül néhány példa következik.

A felhasználó által korábban begyűjtött – és ellenőrzött – nyilvános kulcsok manipulálása, kicserélése útján lehetővé tenni a közbeékelődést.

A felhasználó gépéhez hozzáférve a nem törölt fájlokban megtalálni a kérdéses adatokat. Ugyanott a „törölt” fájlok helyreállításával is elérhető lehet eredmény. A „lomtár ürítése” művelet után a törölt fájlokban tárolt adatok fizikailag még ott vannak a lemezegység szabad adatterületein, amíg újabb fájlok létrehozása során végül ténylegesen felül nem íródnak.

A merevlemezek fizikailag felülírt adatterületéről is visszanyerhető lehet az adat a mágneses jelek szóródásának érzékelésével – ehhez természetesen különleges hardver szükséges.

Hardveres billentyűnaplózó telepítésével különféle, közöttük a titkos kulcsot védő jelszó megszerzésére.

Trójai programok és vírusok és/vagy egyéb szoftveres megoldások, „kémprogramok” segítségével.

A számítógép elektromágneses sugárzásának távolról való érzékelésével és elemzésével.

A számítógép központi memóriája (RAM) a kikapcsoláskor nem azonnal veszíti el

[13] http://enigmail.mozdev.org

tartalmát, a memóriamodulok hűtésével ez a folyamat jelentősen lassítható, így a kikapcsolás után akár percekkel is visszanyerhető a memória korábbi tartalma, benne pl. a titkosított merevlemez eléréséhez szükséges kulcs.

Végül, de egyáltalán nem utolsósorban vegyük számításba az emberi tényezőt is: a felhasználó ügyes becsapása vagy fizikai fenyegetése sem hagyható figyelmen kívül.

5.5 Szabad szoftver vs. üzleti licenc

Ha a biztonságnak tétje van, megfontolandók a szoftverválasztás szempontjai is. A szabad szoftverek esetében a rendelkezésünkre áll a teljes – dokumentált – forráskód, azt megvizsgálhatjuk vagy megvizsgáltathatjuk. Mivel ez esetben a forráskód mindenkinek a rendelkezésére áll, ezért efféle vizsgálódásnak tőlünk függetlenül is ki van téve. Erősen valószínűtlen tehát az, hogy a fejlesztők valamilyen hátsó kaput rejtettek volna el benne. Üzleti szoftverek esetében, a forráskód hiányában meg kell bíznunk a fejlesztő cégben, hogy sem szándékosan, sem pedig fejlesztői hiba következtében nem maradt benne ilyen. Üzleti szoftverek licencszerződéseit olvasgatva azonban azt tapasztalhatjuk, hogy általában ennél jóval kevesebbre sem vállalnak garanciát a szoftverfejlesztők.

Különféle szoftverhibák is lehetnek a biztonság szempontjából kritikus pontok. A forráskód rendelkezésre állása esetén a típusos hibák kereshetők, ellenőrizhetők, a programok tervszerűen tesztelhetők. Forráskód hiányában kizárólag „fekete doboz tesztelés” alkalmazható.

5.6 Adatok megsemmisítése

Az adatok illetéktelen hozzáféréstől való védelme kapcsán fölmerül az adatok garantált megsemmisítésének problémája is, mégpedig kétféle megközelítésben. Egyrészt az adathordozó selejtezése kapcsán, másrészt pedig olyan esetben, ha illetéktelen személy az adathordozó közelébe kerül.

Egy másik csoportosítási mód alapján beszélhetünk az adat megsemmisítéséről az adathordozó üzemképes állapotban való megtartása mellett, illetve magának az adathordozónak a fizikai megsemmisítéséről.

Ha az adathordozót meg kívánjuk tartani, az adathordozó terület olyan felülírását kell megvalósítani, amely kellő biztonságot nyújt a jelmaradványok különleges hardverelemekkel való leolvasása ellen. Például merevlemezek esetén az egyik javasolt – általános – eljárás az első lépésben csupa 0 bittel való felülírás, másodikban a csupa 1 bittel való felülírás, majd további néhány lépésben véletlenszerű bitmintákkal való felülírás. Más források szerint a többszöri felülírásnál alkalmazandó bitminták függnek, vagy függhetnek a merevlemez által alkalmazott mágnesezési eljárástól.

Az adathordozó megsemmisítése célszerűen annak fel- vagy beolvasztása lehet.

6 A magánszféra védelme

Érdemes lehet ezt a területet gondosan tanulmányozni a vállalati adatbiztonság szempontjából is. Egyrészt mert a vállalat alkalmazottai emberek, akik nem választhatók el teljes mértékben munkájuktól és munkahelyüktől, másrészt pedig mert ezt a területet fokozott figyelemmel kísérik az emberi jogokra érzékeny szervezetek és személyek.

Napjainkban a digitális technika fejlődése olyan technikai eszközöket és lehetőségeket teremtett meg, amelyek korábban elképzelhetetlenek voltak. Ismét csak példák következnek, a figyelem felhívása és az érdeklődés felkeltése céljából.

A böngészési szokások vizsgálata elég sokat elárul az emberről, ezen belül is kiemelten a keresései. Számoljunk! Van ma Magyarországon mintegy kétmillió szélessávú internet-előfizetés. Tegyük fel (kissé talán túlbecsülve a tényleges adatokat), hogy az átlagos előfizető (és családtagjai) átlagosan naponta száz oldalt néznek meg. Legyen egy url átlagos hossza 100 karakter. Néhány bájtot igényel az időbélyeg és az előfizető azonosítója. Így összességében kb. 20 GB szükséges az összes előfizető egynapi böngészési adatainak – a felkeresett oldalak címeinek – rögzítéséhez. Egy 2 TB méretű merevlemezen tehát bő három havi adatmennyiség elfér, és kiskereskedelmi áron kb. bruttó 30.000 magyar forintba kerül...

Hasonlóképpen igen olcsón feltérképezhető emberek kapcsolati hálója is. A küldött és kapott emilek tartalmát mellőzve az emilforgalom adatai, illetve a telefonos híváslisták is igen sok dologról árulkodhatnak. A Facebook és az Iwiw pedig tálcán kínál ugyancsak egy csomó értékes adatot a kíváncsi érdeklődőknek. Idén év elején magas rangú NATO-vezető (James Stavridis tengernagy) nevében hamis Facebook-profil létrehozásával számos kollégája személyes adatait sikerült megszerezniük ismeretlen tetteseknek...

Az úgynevezett okostelefonok kémkednek gazdájuk után, a Google a StreetView felvételeinek készítése közben vezeték nélküli hálózatok adatai után is kutatott. Határőrök átkutathatják az USÁ-ba beutazók laptopját, Magyarországon – uniós irányelveket jelentősen túlteljesítve – három évig őrzik az előfizetők kommunikációs profilját (telefonos és internetes kapcsolódási és tartózkodási adatait).

7 Technika, üzlet, jog és etika

Amire megvan a technikai lehetőség, avval számolni kell – számolni kellett

mindig is, mert az adat kincset ér (vö. „információs társadalom). A teljesség igénye nélkül számos példát láttunk arra, hogy milyen veszélyek fenyegethetnek bennünket, és milyen védekezési lehetőségeink vannak.

A biztonságot – legalábbis a számítástechnika és az adatok vonatkozásában – többnyire mint technikai, technológiai kérdésként kezeljük. Mások mellett Bruce Schneier mutat rá arra, hogy a biztonság legalább annyira gazdasági-pénzügyi kérdés is: a problémák jelentős hányada abból fakad, hogy akiknek módjukban áll megvédeni, biztonságossá tenni egy rendszer működését, nem azonosak azokkal, akik a zavarok költségeit viselik. A biztonság, a minőség drága dolog, és a cégek csak annyit költenek rá, amennyit feltétlenül muszáj: amennyit a piaci átlag, az iparági legjobb gyakorlat elvár. Ha a szoftverekre a gépkocsikhoz hasonló fogyasztóvédelmi előírások vonatkoznának, sokkal jobb lenne a minőségük és a megbízhatóságuk.

Jogállamban élünk, azonban senki ne ringassa magát abban az illúzióban, hogy az esetlegesen ellenérdekelt felet ez a körülmény megakadályozza törvénytelen eszközök alkalmazásában. Nem árt azonban ismerni a jogszabályi környezetet, amelyben magánemberként létezünk és alkalmazottként (esetleg cégtulajdonosként) dolgozunk. Néhány fontos jogszabály:

A Büntető Törvénykönyv 300/C. § szól a számítástechnikai rendszer és adatok elleni bűncselekményekről.

A 2011. évi CXII. törvény szól az információs önrendelkezési jogról és az információszabadságról.

A 2001. évi CVIII. törvény szól az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

A 2001. évi XXXV. törvény szól az elektronikus aláírásról.

Van néhány nehézség a jog és az informatika határterületein, amelyekről érdemes lehet elgondolkodni.

Ilyen például az a sajátosság, hogy a személyi számítógépek felépítésének sajátosságai miatt bármiféle, számítógépen talált adattartalom bármire vonatkozó bizonyító ereje – informatikai szempontból legalábbis – megkérdőjelezhető. Az IP cím hálózati eszközt azonosít és nem feltétlenül számítógépet, végképp nem a gép előtt pillanatnyilag ülő embert. Nincs semmilyen technikai garancia arra, hogy egy személyi számítógép teljes mértékben és kizárólagosan gazdája ellenőrzése alatt áll, és senki, semmilyen módon nem férhet hozzá ahhoz. Fokozottan igaz ez, ha hálózatra csatlakoztatott számítógépről van szó.

Ugyancsak érdekes kérdéseket vet föl az internet határokon átnyúló mivolta. Ha egy kiszolgáló gép az A országban van egy szerverfarmon elhelyezve, szolgáltatásait elsősorban a B ország állampolgárai veszik igénybe, miközben üzemeltetését a C országból végzik, akkor milyen jog vonatkozik a fölmerülő

problémákra, és hogyan lehet azoknak érvényt szerezni?

A jogszabályok formális előírások, amelyek a társadalom értékítéletét próbálják tükrözni, több-kevesebb sikerrel és több-kevesebb késéssel. (Vö. az elhíresült mondással: „Lehet, hogy nem etikus, de jogszerű".) Szavazattöbbségre épülő rendszerben nem biztos, hogy minden jogszabály minden körülmény között összhangban van akár a józan ésszel, akár valódi (pl. természettörvényben gyökerező) értékekkel. Éppen ezért az erkölcsi normák fontosabbak minden más szabálynál, ide értve a formális jogszabályokat is, az önérdeknél is, és érvényességük független bármiféle hatósági vagy szervezeti jóváhagyástól. „Vannak íratlan törvények, amelyeket nagyon szigorúan kell venni éppen azoknak, akik az írott törvényeket eredeti merevségükből olykor hajlékonyabbá teszik."

Mivel korunkban nemcsak a digitálisan tárolt és kezelt adatok mennyisége növekszik napról-napra, de a tőlük való függőségünk mértéke is, számos jel szerint paradigmaváltás zajlik éppen, ezért kiemelt fontosságú, hogy „információs társadalmunknak" ép és érzékeny lelkiismeretű polgárai legyünk.

Irodalom

[1] Dwivedi, Hirmanshu: SSH a gyakorlatban, Módszerek biztonságos hálózati kapcsolatok kialakítására, Kiskapu, 2004

[2] Flickenger, Rob: Linux Server Hacks, O'Reilly & Associates, Inc., 2003

[3] Gagné, Marcel: Linux-rendszerfelügyelet, Kiskapu, 2002

[4] Hagen, Bill von – Jones, Brian K.: Linux Server Hacks, Volume Two, O'Reilly Media, Inc., 2006

[5] Koscher, Karl et al.: Experimental Security Analysis of a Modern Automobile, 2010 IEEE Symposium on Security and Privacy, http://www.autosec.org/pubs/cars-oakland2010.pdf

[6] Ködmön József: Kriptográfia, Computerbooks, Budapest, 2002

[7] Nemetz Tibor: Kriptográfiai mondanivaló újonnan beinduló adatvédelmi rendszerek szervezői számára, "Adatvédelem Magyarországon" c. konferencia, Mátraháza, 1995, L. pl. http://193.225.224.240/gazdinfo/gyak_KEA/Nemetz.html

[8] Robinson, Sarah: Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders, SIAM News, Volume 36, Number 5, June 2003

[9] Schneier, Bruce: Applied cryptography: Protocols, algorithms and source code in C. Wiley & Sons, New York, 1996 (2nd ed.)

[10] Schneier, Bruce: Schneier a biztonságról, HVG könyvek, Budapest, 2010

[11] The Free Software Definition, http://www.fsf.org/licensing/essays/free-

sw.html

[12] Tsutomu Matsumoto et al.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, Thursday-Friday 24-25 January 2002, http://cryptome.org/gummy.htm

[13] Vajda – Bencsáth – Bognár: Tanulmány a napvilágra került Elender jelszavakról, a Budapesti Műszaki Egyetem Híradástechnikai Tanszék Üzleti Adatbiztonság Laboratóriumának közleménye, 2000. február 3

[14] Zimmermann, Philip: The official PGP user's guide, MIT Press (Cambridge, Mass), 1996, ISBN 0262740176, Originally part of the PGP program package: ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf