Az elektronikus levelezés fenyegetettsége napjainkban — avagy mit tehetünk a biztonságért

Kóbor András — Gulyás Gábor György — Schulcz Róbert*

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Híradástechnika Tanszék
1117 Budapest, Magyar tudósok körútja 2., I ép. IB 113.
Telefon: +36 1 463–3227, Fax: +36 1 463–3263
e-mail: elvislo@vipmail.hu

Absztrakt

Az elektronikus levelezés az egyik legelterjedtebb internetes tevékenység, mégis a felhasználók többsége nincs tudatában sem a levelező szolgáltatások sebezhetőségének, sem a visszaélési lehetőségeknek, sem pedig a védekezési eszközöknek és módszereknek. A tanulmány bemutatja a levelező rendszereknek a magánélet védelme szempontjából legfontosabb elemeit és szakaszait, az egyes szakaszokban nyíló támadási lehetőségeket, a támadó eszközöket és alkalmazásukat; sorra veszi a levelezésben részt vevő szereplők elvárásait és igényeit, majd áttekinti a felsorolt támadások ellen alkalmazható védelmi eszközöket és módszereket. A szerzők a levelező rendszerek vizsgált attribútumait rendszerbe foglalták és táblázatos formában ábrázolták, végül rámutattak az egymásnak ellentmondó tulajdonságokra is.

Kulcsszavak: *e-mail, privátszféra, internet, spam, cenzúra*

1. Bevezető

Korunk információs társadalmában az elektronikus adatcsere mindennapi életünk szerves részét képezi. Napi egy millió e-mailt küldenek és öt milliót fogadnak Magyarország egyik legnagyobb ingyenes levelezési szolgáltatójánál, körülbelül 1,5–1,7 millió felhasználóval [1]. Ebben a forgalomban nincs benne a kéretlen reklámlevelek, az ún. spam-ek által generált forgalom, de nem ezek jelentik az egyedüli veszélyt postafiókunk számára. Felmerülhet az igény, hogy leveleink tartalmát, levélcímünket, személyes adatainkat, felhasználói

* Kóbor András, a Budapesti Műszaki és Gazdaságtudományi Egyetem ötödéves műszaki informatikus hallgatója; Gulyás Gábor György, a BME Villamosmérnöki és Informatikai Kar Híradástechnikai Tanszékének doktorandusz hallgatója; Schulcz Róbert, a BME Villamosmérnöki és Informatikai Kar Híradástechnikai Tanszékének tudományos segédmunkatársa.

viselkedésünket védjük, illetve az általunk küldött dokumentum, levél, adat forrásának hitelessége egyértelműen megállapítható legyen. Ha ezek illetéktelen felhasználók kezébe kerülnek, akkor azok visszaélésekre, bűncselekményekre adhatnak lehetőséget.

A levelünk tartalmának „elrejtése" az illetéktelenek elől talán az egyik legfontosabb dolog, ami felmerül az elektronikus levelezéssel kapcsolatban. Amikor ugyanis feladjuk levelünket és a világhálón útjára indítjuk, egy rövidebb–hosszabb ideig tartó kézbesítési folyamaton megy keresztül, melynek végén — szerencsés esetben — megérkezik a címzett postafiókjába. Azonban a továbbítás során számtalan szolgáltató eszközén, továbbító szerverén megy keresztül és tárolódik, aminek következtében a hozzáértő, és ilyen aspektusból rosszindulatúnak tekinthető személyek számára rendelkezésre áll. Különböző megoldásokat kell keresnünk, amelynek használatával kódolhatjuk levelünket úgy, hogy azt csak a címzett legyen képes visszafejteni.

Felmerül az igény arra is, hogy valamilyen módon kézjegyünkkel lássuk el saját leveleinket, biztosítva a címzettet, hogy az elektronikus levelet tőlünk kapta. Fontos szempont az is, hogy a sérthetetlenség megmaradjon, azaz levelünk tartalmát mások ne módosíthassák.

Más szempontból nézve fontos, hogy szükség esetén névtelen leveleket is küldhessünk, azaz hogy postafiókunk címe is láthatatlan maradjon azok számára, akikkel nem kívánunk elektronikus levelezést folytatni. Mindennapos dolognak számít, hogy kéretlen leveleket, spam-eket kapunk postaládánkba, de a spam-áradat postaládánkat is megbéníthatja. Egyrészről az ilyen célú védelem, másrészről az anonim véleménynyilvánítás lehetősége miatt tartjuk fontosnak a névtelen levélküldés lehetőségét. Erre nyújtanak megoldást a különböző, névtelenséget biztosító szerverek, illetve eldobható e-mail címek, melyekkel elrejthetjük valódi címünket a jogosulatlan személyek elől.

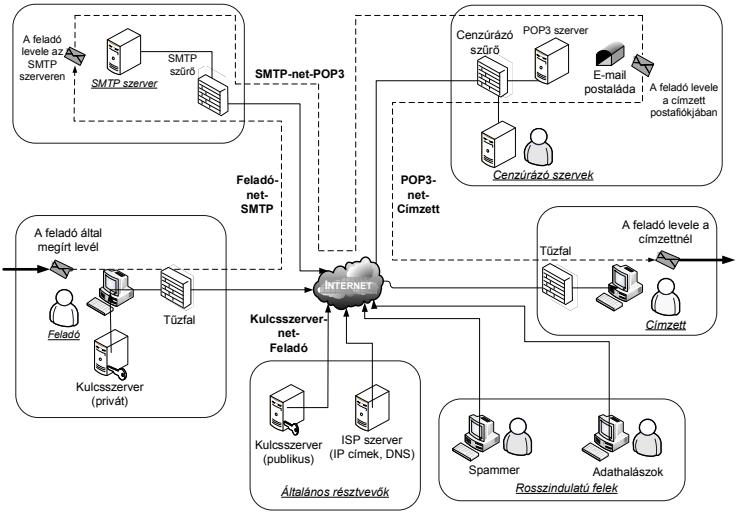
Az anonimitás akkor is lényeges lehet, ha nem akarjuk, hogy a különböző továbbított e-mailek lehallgatása, megszerzése révén valaki a fejrészek alapján kapcsolathálókat építsen ki, vagy profilépítést hajtson végre, melynek következtében célzott hirdetések célpontjává válhatunk. Többféle lehetőség is nyílik arra, hogy az internet adta lehetőségekkel élve levelünket ne közvetlenül, hanem közvetve postázzuk, ezzel is kevesebb helyen felfedve e-mail címünket.

2. Támadó modell

A következőkben bemutatott modellben áttekintjük, hogy milyen veszélyekkel kell szembenéznünk e-mail forgalmunkkal kapcsolatban, milyen szereplőket kell figyelembe vennünk, illetve e szereplők lehetséges céljait is számba vesszük.

2.1. A privátszféra sérülése a továbbítási hálózaton

Amikor az elektronikus levelezés privátszférát érintő kérdéseiről beszélünk, nem csupán azt kell figyelembe vennünk, hogy a feladott levél milyen útvonalon, milyen szereplőket érintve éri el a célját, hanem magával a levél attribútumaival, illetve a levelezéshez kapcsolódó szereplőkkel is szükséges foglalkoznunk.



1. ábra: A szereplők elhelyezkedése és az e-mail továbbítás szakaszai

Az 1. ábrán nyomon követhetjük az elektronikus levél útját a feladótól a címzettig, a hálózat szakaszait és a levelezés szereplőit. A következőkben a különféle szakaszokat tekintjük át a privátszférát érintő hatások szempontjai szerint.

2.1.1. Feladó – net – SMTP szakasz

Ebben a szakaszban jut el a feladó levele a levelezési szolgáltató SMTP (Simple Mail Transfer Protocol) szerveréhez. A levelezési szolgáltatók SMTP szervere port alapú szűrést[1] biztosíthat a spam-ek ellen, ami lehet például IP vagy statisztikai alapú. Levelünk ezen a szakaszon sérülhet, amennyiben a portszűrés alapján spam-nek minősül. Ez kétféle módon lehetséges: egyrészt a kliens oldali munkaállomás fertőzött és önmagától generál spam-eket, másrészt a felhasználó rosszhiszemű e-mail felhasználás esetén tudatosan küld kéretlen leveleket nagy mennyiségben. Mivel levelünk az internet hálózatán kerül továbbításra, ezért ki van téve az ott fellépő támadásoknak (lehallgatás, módosítás). Ha céges hálózatunkból küldünk e-mailt, akár saját SMTP levelezőszerverről, akár nem, akkor a rendszeradminisztrátor bármikor elolvashatja levelezésünket, ha nem alkalmazunk titkosítást.

Az SMTP szervereknél elengedhetetlen továbbá a hitelesítés, ugyanis a spam-ek többsége regisztrálatlan gépekről kerül feladásra. Ez lehet IP-cím szerinti, de a fejlett levelezőszerverek és kliensek más IP-hálózatokból származó levelek küldését is engedélyezik. Erre használatosak a fekete- és fehérlisták: a ezekben a listákban a szerveren megadhatunk SMTP host-okat, ahonnan elfogadunk vagy tiltunk SMTP kapcsolatokat [2].

2.1.2. SMTP – net – POP3 szakasz

Ezen a szakaszon történik a levél továbbítása az interneten keresztül a feladó SMTP szerverétől a címzett POP3 szerveréig. Mivel a továbbítás itt is az interneten keresztül történik, ezért itt is a lehallgatásos támadásokkal, problémákkal kell szembenéznünk: egy támadó lehallgathatja a levelünket a hálózaton, módosítja, majd továbbküldi. Mivel az interneten elérhető levelező szolgáltatások többsége *best-effort* alapú — vagyis nem nyújt garanciát az adatok időben történő és teljes átvitelére, csupán az éppen rendelkezésre álló erőforrások és hálózati állapotok között törekszik a szolgáltatás teljesítésére — az is előfordulhat, hogy levelünk jelentős késéssel, vagy egyáltalán nem ér célba.

Ha olyan levelezési szolgáltatót használunk, amelynek szolgáltatásai nem kerülnek pénzbe, akkor gyakran megeshet, hogy a levéltörzs végére szöveges hirdetések kerülnek (általában pár sor, amit alaposan elkülönít a szolgáltató). Ezen a ponton sérül a levelünk integritása,

[1] TCP portszám alapú szűrés, mivel az SMTP protokoll a 25-ös portot használja, így a levélforgalom leválasztható és vizsgálható.

hirdetéshordozóvá válik, hiszen plusz tartalom került bele, bár ezt elfogadtuk a felhasználási feltételek részeként [3].

2.1.3. POP3 – net – Címzett szakasz

Ezen a szakaszon a levél már megérkezett a címzett postafiókjába, aki letöltheti majd azokat a kliens oldali gépére. A levelezőszolgáltatók szervereinél különböző cenzúrázó szervek (például nemzetbiztonsági szolgálatok) elhelyezhetnek szűrőket, melyek szűrik és elmentik a leveleket, ha azokban bizonyos kulcsszavak vagy mintázatok előfordulnak. Az is előfordulhat (mint például Mianmarban), hogy webalapú email címeket (például a Yahoo Mailt, a Gmailt, vagy a Hotmailt) nem lehet használni. Az internetkávézókban elhelyezett gépek ötpercenként mentik el a felhasználó által felkeresett honlapokat, hogy a hatóságok nyomon követhessék tevékenységét [4]. Enyhébb esetekben — Ukrajnában, Oroszországban, Nagy-Britanniában és Magyarországon — törvényi szabályozás kötelezi az internet szolgáltatókat, hogy megfigyelési lehetőséget nyissanak az adatforgalomra.[2]

2.1.4. Kulcsszerver – (net) – Feladó szakasz (opcionális)

Amennyiben használunk valamilyen titkosítást a levelezésünk folyamán, úgy létrejön ez a szakasz is. A levél titkosításához az interneten (vagy helyi hálózaton, de a legjobb esetben saját számítógépünkön, hiszen ekkor erről a szakasztól nem is beszélhetünk) lévő kulcsszerverek biztosíthatnak nyilvános kulcsokat, melyekkel titkosíthatjuk levelünket úgy, hogy azt csak a címzett legyen képes visszafejteni. Használhatunk saját hardveres kulcsot is, például USB token formájában. Ha esetleg egy támadó kicseréli a nyilvános kulcstárban a kulcsokat úgy, hogy a címzettünk nyilvános kulcsát a sajátjával helyettesíti, akkor a levelünket lehallgatva vissza tudja fejteni az üzenetet.

2.2. A levelezés szereplői és céljaik

Szempontrendszerünk alapján a levelezés szereplőit szándékaik szerint három kategóriába sorolhatjuk, a felhasználóhoz való viszonyuk alapján: semleges, rosszindulatú és jóindulatú. A semleges szereplők általában saját céljaikat igyekeznek elérni, feladatukat teljesíteni, lehetőleg úgy, hogy a többi szereplő céljait, feladatainak teljesítését ne befolyásolják. A rosszindulatú szereplők általában a felhasználók céljaival, privátszféráját érintő rendelkezéseivel, akaratával ellentétes üzleti célokat kívánnak megvalósítani a saját hasznukra. A jóindulatú szereplők a levelezés „tisztaságáért” felelősek. Céljuk, hogy a

[2] Lásd az elektronikus hírközlésről szóló 2003. évi C. törvény vonatkozó rendelkezéseit, valamint az Európai Parlament és a Tanács 2002/58/EK irányelvét, illetve az azt módosító 2006/24/EK irányelvet. – *A szerk.*

semleges felhasználók céljaival egyező módon erősítsék a privátszférájukat a rosszindulatú szereplőkkel szemben. Le kell azonban szögeznünk, hogy a kategóriák nem különülnek el teljesen egymástól, a kategóriák átfedésben is lehetnek egymással, valamint időközben egy–egy szereplő besorolása változhat.

2.2.1. Felhasználó

A felhasználó célja, hogy a levelét sértetlenül (és olvasatlanul) eljuttassa a címzettnek, illetve sértetlenül megkapja más felhasználók leveleit is. Különleges esetekben rosszindulatúvá válhat, ha például a nem neki címzett leveleket akarja elolvasni, vagy kéretlen levelekkel bombázza a többi felhasználót.

2.2.2. Levelezési szolgáltatást biztosítók

Általános levelezést biztosító szolgáltatók: alapvetően semleges szereplő. Közvetve rosszindulatúvá válhat, ha egy spam-küldő felhasználó vagy rosszindulatú program felhasználja az SMTP szerver nyitott portját, és kéretlen leveleket küld a felhasználóknak.

Anonim levelezést biztosító szolgáltatók: alapvetően jóindulatú szereplő. Céljai közé tartozik a levél feladójának anonimizálása, valamint a levél visszakövethetetlenné és/vagy megfejthetetlenné tétele a rosszindulatú szereplők számára.

2.2.3. Az internet szolgáltató

Alapvetően semleges szereplő. Mivel annak nyújt szolgáltatást, aki teljesíti a piaci feltételeket, ezért a rosszindulatú szereplők is a szolgáltató közvetítésével végzik tevékenységüket. Rosszindulatúvá válhat, ha kiadja az ügyfelei, előfizetői adatait arra nem jogosultaknak, illetve nem biztosítja ezen adatok megfelelő védelmét. Például a versenyszférában tőkét kovácsol előfizetői személyes adataiból. Ha nincs kimondottan előfizetőre vonatkozó adatkezelői előírás, akkor a szolgáltató a szerződés megszűnésétől számított egy év egy hónapig tárolhatja előfizetői adatait [5].

2.2.4. Adatvédelmi biztos (adatvédelmi hatóság)

Alapvetően jóindulatú szereplő. Célja, hogy a felhasználók személyes adatainak védelmét szolgálja, és a felhasználók szempontjait képviselje, érvényesítse a nagyobb vállalatokkal vagy szervezetekkel szemben. Az adatvédelmi biztos Magyarországon előzetes bejelentés nélkül beléphet bármilyen helységbe, ahol adatkezelés folyik [6]. A biztos minden adatkezelést jogosult megvizsgálni, függetlenül attól, hogy az adatkezelő állami,

önkormányzati, vagy a magánszférába tartozik-e. Például ellenőrizheti az internet szolgáltatókat, hogy megfelelően kezelik-e előfizetőik adatait.

2.2.5. Üzleti célú felhasználók: direkt marketingesek, hirdetők, profilépítők

A spam-eket küldési típusuk szerint itt két csoportra oszthatjuk: az *opt-out* (leiratkozás lehetőségével) és az *opt-in* (felhasználó engedélyével) típusúakra. Az *opt-out* rendszert sokan hibáztatják, mivel a fogadóra terhel bizonyos feladatokat (a leiratkozást), illetve a spammer akár egy másik email-címről folytathatja a tevékenységét, mivel a leiratkozás csak az adott címre vonatkozik. Az erre vonatkozó magyar törvény főszabálya szerint csak *opt-in* módon küldhető elektronikus üzleti reklámlevél.[3]

Felhasználó engedélyével üzenetet küldő: alapvetően semleges vagy jóindulatú szereplő. Célja lehet például, hogy minél több felhasználónak értékesítse a termékeit, szolgáltatásait, úgy, hogy az a vevőnek is a lehető legkedvezőbb legyen (személyre szabott ajánlatok, kedvezmények, stb.).

Felhasználó engedélye nélkül üzenetet küldő: a felhasználó szempontjából alapvetően rosszindulatú szereplő. Célja, hogy minél több „élő", működő postafiókot árasszon el kéretlen reklámanyagokkal.

A *direkt marketinggel foglalkozók* (közvetlen üzletszerzők) megpróbálják termékeiket értékesíteni minél több felhasználó számára. Lehetnek kereskedők, webes üzlet tulajdonosok, stb.

A *hirdetők* célja, hogy minél több létező, működő postafiókot lehetőleg minél több hirdetéssel árasszanak el. Ezt tehetik direkt marketingesek megbízásából is.

A *profilépítők* megpróbálnak minél több felhasználóról minél pontosabb információkat szerezni, mint például az internetezési szokások, érdeklődési kör, személyes információk, majd ezeket értékesíteni.

[3] Lásd erről az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, az elektronikus hírközlésről szóló 2003. évi C. törvény, illetve a gazdasági reklámtevékenységről szóló 1997. évi LVIII. törvény vonatkozó rendelkezéseit. – *A szerk.*

2.2.6. Adathalászok

Alapvetően rosszindulatú szereplők. Céljuk, hogy másnak tűnve a felhasználók szemében kicsalják személyes adataikat, hozzáféréseiket, melyeket aztán felhasználhatnak tipikusan pénzszerzés céljára (banki számlaadatok megadása, „adakozás" stb.). Az adathalászat új formája az ún. „whaling[4]", amelyben az adathalászok kifejezetten céges vezetőkre, „nagy halakra" specializálódnak.

2.2.7. Cenzúrázó szervek

Alapvetően semleges szereplő, de bizonyos országokban negatív szereplőként is tekinthetünk rá. Célja, hogy különböző, általa meghatározott tartalmak terjedésének gátat szabjon. Nézőpont kérdése, hogy rosszindulatúnak fogjuk-e fel, ha valamilyen általunk legálisnak vélt tartalmat blokkol, illetve felfoghatjuk jóindulatúnak is, ha a legitim többség által illegálisnak tartott tartalmak ellen lép fel. Ide sorolhatjuk például a munkahelyi cenzúrát is.

Kínában a feltételeket rögzítő dokumentumot és az ezzel kapcsolatos megállapodást írtak alá az Internet Society of China (ISC) és az országban tevékenykedő 21 kisebb-nagyobb szolgáltató, köztük a Yahoo és a Microsoft is [7]. Ennek értelmében a blog oldalakat és egyéb szolgáltatásokat nyújtó cégek rögzítik a naplót vezetők és a bejegyzésekhez hozzászólók adatait, amelyeket azután szükség esetén a hatóságok rendelkezésére bocsátanak.

3. Eszközök

Ebben a szakaszban röviden bemutatjuk, hogy milyen eszközök állnak rendelkezésére egy rosszindulatú szereplőnek, illetve bizonyos országokban a cenzúrázó szerveknek.

3.1. Spam-ek

A *spam* olyan kéretlen reklámlevél, amelyet a felhasználó úgy kap meg elektronikus levélcímére, hogy előzőleg nem kérte, illetve nem adott engedélyt annak küldésére. Az első elektronikus spam-et már 1978. május 3-án elküldték, ez a *DEC spam* [8]. Innentől számítjuk a valódi spam-korszakot, amely napjainkig tart. A probléma azonban csak 1993. óta igazán jelentős. Az első vállalat, amely spam-et küldött, a Canter & Siegel volt, ők

[4] A „phising", az adathalászat analógiájára magyarra fordítva talán a bálnavadászat lenne a megfelelő kifejezés.

1994. április 12-én küldték el a hírcsoport spam-jüket. Az alábbi spam-típusokat a Spamwiki honlapról gyűjtöttük össze [8].

3.1.1. E-mail alapú kéretlen reklámlevelek

Ebbe a kategóriába soroljuk többek között a *klasszikus szöveges e-mail spam-et,* amely az egyik legrégebbi típus. A levél törzsében szöveg formájában jeleníti meg a hirdetést. Ide tartozik továbbá a *képes spam, amely* a szöveges törzsbe beágyazva, képként jeleníti meg a hirdetést, melynek következménye, hogy az anti-spam programok nehezebben szűrik ki. Az egyik legfrissebb típus a *PDF spam*, amely egy hirdetést tartalmazó pdf csatolmányú levél. A másik legfrissebb típus az *MP3 spam,* amely 2007-es év legutolsó spam-típusa. A létrejöttének az alapja az, hogy az emberek szívesen küldenek egymásnak hangfájlokat. Ha egy felhasználó MP3 spam-et kap és lejátssza, akkor egy gépi hang elbetűzi a cég nevét, majd az ajánlat lesz hallható.

3.1.2. Egyéb, számítógépes közegben terjedő spam üzenettípusok

Nem közvetlenül e-mailben vagy csatolmányként terjednek, hanem weboldalakon, fórumokon találkozhatunk velük. Ebbe a csoportba tartozik a *chat spam,* amely az internetes csevegő szolgáltatásokon keresztül küldött spam. Egy felhasználónak álcázott spambot[5] bizonyos hirdetéseket küld egymás után többször vagy több beszélgető szobába, amelyet a szobában tartózkodók látnak, néha pedig privát beszélgetést is kezdeményez, és oda küldi el a hirdetést. A következő típus ebben a kategóriában a *fórum spam,* amely olyan spam, melyeket a témától függetlenül internetes fórumokra küldenek, esetleg van egy olyan külön témakör, melyet valaki a saját reklámozására nyitott. Létezik továbbá *hírcsoport spam* is, amely olyan spam, melyet egy hírcsoportra küldenek. Az esetek többségében a spammer maga készíti a bejegyzést, de előfordulhat, hogy spambot segítségével hagy üzeneteket. Meg kell említenünk az *IP spam-et,* amely a Windows operációs rendszerek automatikus üzenetszolgáltatásán keresztül küldenek. Az egyik legújabb és legérdekesebb típus a *közösségi hálózati spam,* amely a hálózati közösségépítő oldalakon történő reklámozást jelenti.[6] Ez történhet úgy, hogy megszerzik egy felhasználó fiókját, majd az ő nevében küldik szét a hirdetéseket. Az utolsó spam-fajta a csoportban a *vendégkönyv spam,* amely a spamdexing (internetes keresők „spam-elése" a jobb találati arány érdekében) egyik technikája, mely során az egyes weboldalakon található vendégkönyvekbe küld spam-et valaki.

[5] A spam tevékenységgel kapcsolatba hozható programokat hívjuk így. Ilyen például a webet böngésző, e-mail címeket gyűjtő program is.

[6] A magyar közösségi oldalakon megjelenő spam-ekről a *PET Portál és Blog* is tudósított [9]

3.1.3. Egyéb spam-ek

Az érdekesség kedvéért megemlíthető még két, nem számítógépes spam: a *mobil spam,* amelyet mobiltelefonra küldenek, általában SMS formájában, és a *junk fax* vagy *faxspam* melyet faxon keresztül küldenek.

3.2. Malware, spyware, vírusok

A címben említett rosszindulatú szoftvereket vizsgáljuk meg az alábbiakban az elektronikus levelezésre vonatkozó hatásuk szempontjából. Ezeket arra használják, hogy megismerjék bizonyos személyes szokásainkat, információinkat, melyekből aztán hasznot húzhatnak, illetve számítógépünket felhasználják interneten elkövetett bűncselekményekhez, például spam-küldő hálózatot építsenek ki. A működésük szerint az alábbi három csoportba oszthatjuk őket.

Malware-nek nevezzük azokat a programokat, amelyek a felhasználó tudta nélkül beépülnek az egyes rendszerekbe és károsíthatják azokat. Nem minden malware feltétlenül káros hatású, a kimondottan rombolási céllal létrehozott kódokat a *badware* kifejezéssel illetik. Az alábbi két csoport tehát ebbe a kategóriába tartozik.

A *számítógépes vírus* olyan önsokszorosító program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban, valamint az esetek többségében a felhasználó tudta nélkül fut. Tehát terjedésükhöz szükséges valamilyen más közeg is (dokumentum, program), amelyhez „hozzákapcsolódhat". Ilyenek például a *trójai lovak,* melyek e-mail csatolmányban is terjedhetnek, miközben rendszerinformációkat és e-mail címeket továbbítanak a fertőzött gépről (például a Trojan.Peacomm.D). Léteznek olyanok is, amelyek feltelepülve távoli szerverekről töltenek le tartalmakat, és kihasználják a számítógép távoli sebezhetőségét (például a Trojan.Pidief.B).

A *számítógépes férgek* a vírusok egyik alosztályát alkotják, amelyek képesek arra, hogy a felhasználók közreműködése nélkül terjedjenek és mutálódjanak, például egy e-mail postafiók címlistájában szereplő összes címre elküldik önmagukat [10].

Spyware-nek nevezzük az olyan, főleg az interneten terjedő számítógépes programok összességét, amelyek célja, hogy törvénytelen úton megszerezzék a megfertőzött számítógép felhasználójának bizonyos személyes adatait, beállításait és feltérképezzék a felhasználási szokásait.

3.3. Cenzúra

Egyes országokban cenzúrázó szervek szabályozhatják az internet- és e-mail forgalmat. E-mail cenzúránál lehetőség van a levelezési szolgáltatók internet-hozzáférési pontjánál bizonyos szűrők elhelyezésére, melyek a levél tartalmát vizsgálva blokkolhatják vagy elmenthetik a levelet. A szűrő elhelyezéséhez természetesen szükségesek a megfelelő (törvényes) jogosultságok is.

3.4. Denial of Service

Ez a támadási fajta a célszámítógép (rendszer) működését hivatott meggátolni, méghozzá oly módon, hogy elárasztja azt feladatokkal, amíg a túlterhelés következtében le nem áll az adott szolgáltatás (rendszer). DoS támadás alá vonható még a szolgáltató vírusvédelmi e-mail átjárójának elárasztása vírusos és nem vírusos levelekkel, továbbá az átjáró elárasztása olyan formailag hibás levelekkel, amelyek megbénítják az átjárót.

3.5. Levelek feladójának hamisítása

Ez a támadási fajta az e-mail feladóját hamisítja, ezzel segítve elő a cím megszerzését. Ezt nevezzük *e-mail spoofing*-nak. A hamisított üzenet (spoofed message) kézhezvételekor a címzett könnyen azt hiheti, hogy a levél olyasvalakitől érkezett, akivel ő valóban kapcsolatban áll, és valószínűleg válaszol is rá. A hamisított e-mailt legkönnyebben egy (általában régi verziójú) open-relay SMTP szerver segítségével lehet küldeni, de a célra alkalmasak lehetnek zombi számítógépek is.

3.6. Zombi hálózatok

A zombi hálózat számítógépek, feltört hálózatok egy csoportja, amely titokban használható rosszindulatú célokra, például túlterheléses támadásokra. Az ilyen hálózatok bérbe adhatók spam-ek ideiglenes küldésére is. Létrehozásukra rosszindulatú kódokat „engedtek szabadon” az interneten, melyek legtöbbször a hálózat, programok ismert gyengeségeit, illetve az IRC csatornákat használják ki, hogy megfertőzzék a számítógépeket.

A legveszélyesebb ezekben a botnetekben az, hogy ha egy rosszindulatú szereplő (hacker[7]) addig még ismeretlen kóddal fertőz meg több ezer, vagy még több számítógépet. Így egy új zombi hálózatot hoz létre, akkor ezeket a vírusirtók nagy valószínűséggel nem szűrik ki, és egy szolgáltató sem áll ellen ilyen méretű DDoS támadásnak[8] (levelezés, banki szolgáltatások, kormányzati szervek, stb.). Az aktiválásuk pillanatáig pedig a zombi gépek teljesen ártalmatlannak tűnnek, így előre igen nehéz felfedezni az újabb hálózatokat.

4. Megvalósítás

Ebben a részben a támadó eszközök különböző felhasználási módjai közül mutatunk be néhányat, kihangsúlyozva az elektronikus levelezéshez való viszonyukat.

4.1. Jogosulatlan adatszerzés, adathalászat (phishing)

A *phishing,* jelszó- vagy adathalászat lényege, hogy valaki úgy szerzi meg egy felhasználó titkos jelszóit, személyes adatait, hogy a felhasználót félrevezetve kicsalja azokat tőle. Az egyik leggyakoribb adathalászati módszer az álnéven írt e-mail, például a címzett bankjának a nevében.

4.2. Profilozás

A módszer lényege, hogy személyes jellegű információkból tematikus ízlés, vagy egyéb célú profilt építsen fel a rosszindulatú fél, amit ha nem is tud egy személyhez, de egy azonosítóhoz, például e-mail címhez köt. Így az egyes felhasználóknak csak olyan tartalmú spam-et küld, mely nagy valószínűséggel felkelti az adott személyt érdeklődését. A profilt a különböző oldalakon megadott adatok alapján állítják össze. A profilokat adatbázisokban gyűjtik. Ha több ilyen adatbázis létezik, akkor ezek között elég gyakori lehet a csere, a felhasználók profiljai pénzért vagy más profilokért cserélhetnek gazdát. Elképzelhető az is, hogy egy rosszindulatú szereplő feltör egy adatbázist, amely jelentős számú személyes adatot tartalmaz. Személyes adatokat könnyen közösségi oldalakról is összegyűjthet, amelyekhez ha e-mail cím is társul, akkor a rosszindulatú szereplő máris elérte célját [11].

[7] A „hacker” kifejezést Magyarországon gyakran tévesen azonosítják az eleve kártékony, rosszindulatú számítógépes kalózzal, a „cracker”-rel, noha a hacker inkább a szabályokat, korlátokat felrúgó, a programok gyengeségeit kipellengérező, a védelmi rendszereket virtusból feltörő afféle „internetes szabadsághős”. – *A szerk.*

[8] Distributed Denial of Service: olyan támadás, melynek során a célpont elosztottan, több számítógépről, rendszerről van kitéve a támadásnak.

4.3. E-mail címszerzési módszerek

Postafiók felderítése olvasási visszaigazolással: ezzel a megoldással olvasási visszaigazolás kérhető az e-mailekre. Ezt felhasználva egy spam küldője könnyedén ellenőrizheti azt, hogy az adott postafiók él-e, hiszen elég, ha a címzett megnyitja a levelet, és elfogadja a visszaigazolás küldését. Ekkor a visszaigazolás fejlécében elküldik az olvasó gépének nevét, IP-címét, az olvasás idejét (a fogadó gépe szerint). Bizonyos esetekben a spammer azzal is megelégedhet, ha nem jön vissza a levelezőszervertől olyan generált levél, hogy az adott postafiók nem létezik. Innentől fogva a címet létezőnek lehet minősíteni.

Hírcsoportokból, levelezési listákból megszerzett e-mail címek: ennél a címszerzési módszernél a spammer a hírcsoportok tagjainak küld spam-et, akik önként adták meg e-mail címüket, amikor a csoportra feliratkoztak. A levelet a spammer természetesen nem csak egy hírcsoportba juttatja el, hanem igyekszik a newsgroup[9] vagy levelezési listákat nyújtó szolgáltatás minden csoportját elérni.

Illegális címlistákból megszerzett e-mail címek: a legtöbb spam illegális címlistákon keresztül érkezik a postafiókunkba. Ennél a módszernél a spamer elindít egy robotot a weben, amely az oldalakon megjelenő e-mail címeket gyűjti össze.

Regisztrációnak álcázva: ebben az esetben valamilyen tartalomhoz csak úgy juthat hozzá a felhasználó, ha egy látszólag könnyed regisztrációt elvégez. Ekkor ismét csak saját maga adja meg az adatait és az e-mail címét. Még az is lehet, hogy a regisztrációs oldal alján kis betűvel ki van írva, hogy az adatokat felhasználják további célokra, de ez elkerülheti a felhasználók figyelmét. Ez még a kedvezőbb eset, hiszen így a felhasználó még kap is valamit a regisztrációért cserébe, ám az is elképzelhető, hogy tartalom szempontjából egy üres oldalon kérik fel az illetőt az adatai megadására, csábító tartalmakat ígérve cserébe, majd az oldal menti az adatokat, de a felhasználó semmit sem kap.

Közösségi portálokról: egy spamer a közösségi portálokról is viszonylag könnyedén megszerezhet jelentős mennyiségű e-mail címet. Nem kell hozzá mást tennie, mint regisztrálni az adott portál honlapján, lehetőleg valami hangzatos gyűjtőklub névvel, majd minél több felhasználót véletlenszerűen bejelölni. A felhasználók egy része valószínűleg visszaigazolja a jelölést, és ezek után láthatóvá válik az e-mail címük.

[9] Hírcsoportok. Nyilvános helyek az interneten, ahol tematikusan rendszerezett üzenetek helyezhetők el és olvashatók.

Brute force módszer: a támadó megpróbálkozhat olyan támadás kivitelezésével is, amely egy adott szolgáltató e-mail címeit próbálgatja végig karaktergenerálással. Például a Vipmail.hu e-mail szolgáltató postafiókjait végigpróbálgatja oly módon, hogy a @vipmail.hu elé generál lehetséges fiókokat valamilyen szisztéma szerint (szótár alapján vagy véletlenszerűen), és azoknak levelet küld (csoportosan). Ahonnan nem pattant vissza a küldött e-mail, az létező postafiók.

E-mail címek fejlécekből: ha kicsit cselesebb a támadó, akkor elképzelhető olyan módszer is, hogy aláírásokat gyűjt e-mailben (vagy valamilyen weboldalon) egy „nemes cél" érdekében. A felhasználó gyanútlanul aláírja, majd továbbküldi a levelet ismerőseinek, majd ha összegyűlik a megfelelő számú aláírás, az utolsó felhasználó visszaküldi a levelet a megadott e-mail címre. Ilyenkor a fejléc és a törzs is megőrzi a címeket, amelyekre a levél továbbítódott. A spammer-nek pedig nincs más dolga, mint hogy felhasználja ezeket.

5. A szereplők elvárásai, igényei

Az itt felsorolt tulajdonságok lehetnek személyhez kötöttek, de lehetnek egy adott felhasználói csoport elvárásai is, például a címzetthez való eljuttatás egyaránt a feladó és a címzett igénye is.

5.1. Integritás, letagadhatatlanság, hitelesség

Az, hogy egy üzenetről meg tudjuk állapítani, hogy biztosan nem sérült az átvitel során, illetve biztosan az adott felhasználótól kaptuk, az egyik legfontosabb elvárás (hitelesség). A legkönnyebben megvalósítani az integritást és a letagadhatatlanságot (vagyis az azonosítást mások számára) a digitális aláírás alkalmazásával lehet.

5.2. Bizalmasság

A másik fontos elvárás az e-mail üzenetekkel szemben, hogy biztosak lehessünk benne, hogy más rosszindulatú szereplő nem fért hozzá. Ezt legkönnyebben titkosító eljárások alkalmazásával érhetjük el.

5.3. Címzetthez való eljuttatás

A levél címzetthez való eljuttatása szintén fontos elvárás lehet a továbbításánál, hiszen a feladónak esetenként biztosnak kell lennie abban, hogy a címzett biztosan elolvasta az üzenetét. Ennek a legegyszerűbb módja az előzőekben bemutatott olvasási visszaigazolás

alkalmazása. A címzetthez való eljuttatás egyéni és csoportos érdek is, hiszen a feladó és a címzett már alkothatnak egy kommunikációs csoportot, így mindkettőnek érdeke, hogy az üzenetek célba érjenek.

5.4. Anonimitás biztosítása

Névtelenségünk megőrzése fontos lehet, ha a címzett elől el akarjuk fedni valódi e-mail címünket és azonosságunkat. Erre többféle módszer létezik. Egyrészt vannak webes felületű, ún. anonim remailer-ek, amelyek csak a címzett e-mail címét és az üzenet törzsét várják el, hogy megadjuk, majd a szolgáltató címével küldik el üzenetünket a címzettnek.

Vannak fejlettebb, Mixmaster, illetve Mixminion típusú anonim remailer-ek, amelyek egy adott hálózaton véletlenszerűen végigküldve és titkosítva az üzenetet megakadályozzák annak visszakövethetőségét (lásd később). Léteznek továbbá olyan szolgáltatások, amelyek elrejtik IP-címünket, a feladás dátumát és a kliens információkat a címzett elől, de általában ezt a szolgáltatást a remailer-ek is nyújtják, nem választható el a kettő egymástól.

6. Védelmek

A felsorolt támadási eszközökkel és módszerekkel szembeni védelmi megoldásokat alapvetően két osztályba, az aktív és passzív védelmek osztályába sorolhatjuk. A passzív védelmeket általában elégséges egyszer vagy ritkán konfigurálni, míg az aktív védelmek esetében léteznek algoritmusok, ám ezeket minden esetben különböző jellemzőkkel alkalmazhatjuk (pl. támadó visszakövetése).

6.1. Spam-ek ellen

A legegyszerűbben úgy védekezhetünk a spam-ek ellen, ha tudatos felhasználói magatartást tanúsítunk: vagyis ne adjuk meg az e-mail címünket mindenféle weboldalon, a teljesen ismeretlen feladójú leveleket megnyitás nélkül töröljük, a csatolmánnyal rendelkező leveleket pedig óvatosan kezeljük, valamint ne iratkozzunk fel nem teljesen megbízható levelezési listákra!

A másik lehetséges védekezési mód a spam-ek ellen a spam-szűrők használata. A statisztikai alapon működő szűrők a szövegekben lévő szavakat, kifejezéseket könnyen szűrik, ám ha a csatolmányban van a reklámanyag (pl. képként), akkor az egyszerű szövegelemző módszerek helyett más megoldást kell keresni.

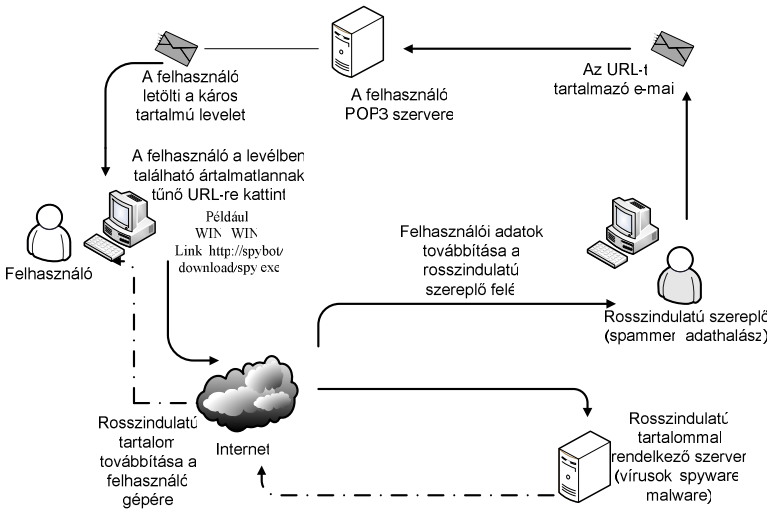
6.2. Malware, spyware, vírusok ellen

Bemutatunk néhány módszert, melyekkel részben védekezhetünk a badware-ek ellen, de mint tudjuk, tökéletes védelem nem létezik.

Kliens oldali megoldások: a számítógépünket a kártékony programok, vírusok és kémprogramok ellen szintén a tudatos magatartással védhetjük meg első fokon. Az első lényeges dolog, amire minden felhasználónak ügyelnie kell, hogy ne kattintson felugró (pop-up) ablakokra a böngészőnkben. Ezeket általában ártó céllal hozzák létre, és az a jobbik eset, ha csak valamilyen „megnyerő" tartalommal bíró oldalra navigál. Ugyanis az egérkattintással URL-eket[10] nyithatunk meg, melyek észrevétlenül káros tartalmat töltenek le számítógépünkre. Ezek ellen bizonyos mértékig védekezhetünk a szoftveres és hardveres tűzfalakkal. A második fontos teendő, hogy mindenképpen legyen antivírus-program telepítve a számítógépre, melyek ideális esetben kiirtják a vírusos állományokat. Rendszeres időközönként anti-spyware programok futtatása is nélkülözhetetlen, mert megeshet, hogy a vírusirtó nem szűri ki a spyware-t. A negyedik fontos momentum, hogy a levelek csatolmányait óvatosan kezeljük! Csak megbízható forrásból származó csatolmányt nyissunk meg. Ugyanez vonatkozik a levelekben található URL-ekre.

Szolgáltató oldali megoldások: a szolgáltatói oldalon is védekezni kell a vírusok, rosszindulatú programok és a jogosulatlan adatszerzésre irányuló betörések ellen. A vírusok elleni védelemre szintén a vírusirtók nyújtanak megoldást, amelyeket különböző szolgáltatást nyújtó szerverekre optimalizáltak. Mivel általában a szolgáltatói oldalon nincs web böngészés és e-mailek megnyitása, ezért a közvetlen URL-eken keresztül történő letöltés valószínűsége is kisebb. Azonban a szervereket is védeni kell tűzfallal a behatolások, támadások ellen.

[10] URL: Uniform Resource Locator, hálózaton használt címmeghatározási séma, amely a hálózaton lévő információk elérési módját és helyét adja meg.



2. ábra: Rosszindulatú URL-t tartalmazó e-mail küldése és megnyitása

6.3. Levelek módosítása ellen

Levelek módosítása ellen a legjobb védelem a digitális aláírás vagy titkosító technikák használata, így a módosítás vagy detektálható, vagy eleve lehetetlen. Az egyik legismertebb a PGP (Pretty Good Privacy), mely e-mailek titkosítására is alkalmas, egy úgynevezett digitális buborék módszer segítségével történik: az üzenet rejtjelezése először egy frissen generált szimmetrikus kulccsal, aztán a szimmetrikus kulcs kódolása a címzett nyilvános kulcsával (mely rendelkezésre állhat valamely kulcstárból), utána a rejtjelezett üzenet elküldése a rejtjelezett szimmetrikus kulccsal.

6.4. DoS és DDoS ellen

A Denial of Service támadások ellen úgy védhetjük a szolgáltatást, hogy megfelelő tűzfalat használunk, továbbá csak a megfelelő portokat engedélyezzük. Az elárasztásos támadás ellen az egyetlen védelem az, ha ki tudjuk szűrni a támadó forgalmát az összes forgalom közül (összes forgalom egyenlő a legitim forgalmak plusz a támadó forgalma). Ha azonban a szűk keresztmetszetet közvetlen internet-kapcsolatunk jelenti, úgy a fogadó oldali szűrés hasztalan: a szűrést ott kell elvégezni, ahol még elég hálózati kapacitás áll rendelkezésre a

legitim és támadó forgalom egyidejű érkeztetésére. Ennek megfelelően az ilyen jellegű védekezés igen nehéz, vagy akár lehetetlen akkor, ha a védelmet csak a fogadó fél oldalán kívánjuk kiépíteni [12]. A vírusvédelmi e-mail átjáróval is DDoS támadás ellen lehet védekezni. Ha egy levél vizsgálata meghalad egy adott kvótát, akkor a levelet nem vizsgálja tovább, hanem vagy eldobja, vagy további vizsgálatra karanténba helyezi.

6.5. Támadó visszakövetése a kliens által

Ha spam-et kaptunk, és ki szeretnénk deríteni, hogy kitől is kaphattuk, akkor tanulmányozzuk át részletesen a fejlécet, amelyből kiderülhet a feladó kiléte! Egy „received" bejegyzés található benne, valamint „message ID", továbbá feladó, címzett és tárgy, valamint a dátumok. Ha több „received" mező található benne, akkor már kezdhetünk gyanakodni. Az egyik leggyakoribb spamer eljárás, hogy az SMTP open relay portokat kihasználva továbbküldik a levelet, mintha nem is tőlük, hanem egy másik szolgáltatótól érkezett volna. A módszer nem célravezető akkor, ha egy botnet-ből érkezett a levél, hiszen ilyenkor gyakorlatilag lehetetlen megtalálni a valódi feladót.

6.6. Kliens (küldő) visszakövethetetlensége

A kliensek visszakövethetetlenségére használható a fentebb említett módszer, miszerint a szolgáltatók open relay SMTP portjait kihasználva és sorozatosan átadva a levél továbbítását, elrejthető a feladó forrása.

A másik lehetőség az anonim remailer-ek használata, melyek segítségével megőrizhetjük névtelenségünket. A módszer lényege, hogy egy titkosított csatornán csatlakozunk a kiszolgálóhoz, amely kiveszi az összes kliens információt a levélből és a saját információival helyettesíti azt.

Egy további lehetőség a Mixminion protokoll használata, amely anonim módon képes üzeneteket fogadni és továbbítani [13]. A protokoll egy kevert hálózati architektúrát használ, hogy erős anonimitást biztosítson. Néhány „önkéntes" szervereket üzemeltet („mix"-ek), amelyek fogadják az üzeneteket, dekódolják, újraütemezik és újraadják őket. Az nem fordulhat elő, hogy a feladó és a címzett között csak egyetlen mix-en keresztül menjen az üzenet. A protokoll az üzenetet szabványos méretű csomagokra bontja, majd minden egyes csomagnak meghatározza az útját a mix hálózaton keresztül. A szoftver kódolja a csomagokat minden szerver nyilvános kulcsával egytől egyig. Ha egy csomag továbbításra kerülne, a Mixminion elküldi az első mixnek, amely dekódolja, megnézi, hogy melyik mix lesz a következő fogadó, majd elküldi a csomagot. Ha a csomag az utolsó mix-

hez ért, akkor az továbbítja a címzetthez. Mivel az összes mix csak a közvetlen feladót látja (akitől előzőleg kapta a csomagot), ezért a csomag visszakövetése lehetetlen. Erre egy implementációt ismertet [14].

6.7. Levelezési szolgáltatók védelme

A szolgáltatók védelmére elhelyezhetünk a szerver közelében ún. „mézescsuprokat" (honeypot). Ezek a rendszerek valamilyen operációs rendszert és szolgáltatást szimulálnak primitív módon. Igazából semmilyen feladatot nem látnak el, ám elhitethetik a támadóval, hogy az a valódi szervert érte el, és így, az álca támadásával egyrészt a támadó szándékára, technikájára, módszereire derülhet fény, s így lehetőség nyílik a valódi rendszer támadásra való felkészítésére. Eközben az eredeti szolgáltatás nem sérül, azonban a nyomok az előbb említett okok mellett megkönnyíthetik a támadó felderítését is.

Az SMTP szerverek védelmére alkalmaznak SMTP portszűrőket, hiszen az open relay-nek köszönhetően ezek nyitva állnak a levelek küldésére, ezért elvileg bárki felhasználhatja őket levelek továbbküldésére. Az SMTP szűrő lehet IP-alapú, amely csak egy megadott címtartományból érkező leveleket továbbítja, illetve amennyiben hozzáfér a levéltörzshöz, akkor statisztikai szűrés is elképzelhető.

6.8. Internet szolgáltatók védelme

Az internet szolgáltatók védelmét a hálózathasználati irányelvek elfogadtatása és betartatása jelenti az összes előfizetővel. Ez tartalmazza az elektronikus levelezésre, a kapcsolattartásra, az osztott erőforrásokra és a hálózathasználatra vonatkozó irányelveket. Amennyiben ezt valamelyik előfizető megszegi, úgy az eset jogi útra terelhető, és akár az előfizető a szolgáltatásból kizárható [15].

7. Osztályozási modellrendszer

Az *1. táblázatból* látszik, hogy igen sokféleképpen védhetjük számítógépünket és levelezésünket különböző helyeken és különböző eszközökkel. Természetesen az is fontos, hogy hol kezdjük el kiépíteni a védelmet. Lehetséges például, hogy ha saját e-mail szerverrel rendelkezünk, akkor már ott elkezdjük szűrni a gyanúsnak tűnő leveleket, így azok a gépünkön már nem okozhatnak problémát.

7.1. Adatvédelmi attribútumok áttekintése

Hitelesség biztosítása: digitális aláírással és hiteles e-mail címmel.

Anonimitás biztosítása: a felhasználó személye nem köthető az e-mail rendszerben használt azonosítókhoz, akkor sem, ha bizonyos azonosítók, pl. IP-cím, e-mail cím, rendelkezésre állnak. Ha a felhasználó ebben az esetben valamilyen pszeudonim azonosítóval van ellátva, akkor előzményekhez, vagy más jelenlévő azonosítókhoz ez nem köthető.

Pszeudonimitás: a felhasználó személye most sem derülhet ki, de egy másik, rendszerben használt azonosítóhoz köthető, amely már magában foglal bizonyos előzményeket. Tehát a pszeudonim azonosító olyan alfanumerikus karaktersorozat, amely alapján nyomon követhető egy adott személy tevékenysége, bizonyos cselekvései, köthetünk hozzá másik rendszerből származó azonosítókat (például e-mail cím), de személyes információkat nem, vagy csak nagyon nehezen kapcsolhatunk hozzá.

Összekapcsolhatatlanság biztosítása: az összekapcsolhatatlanság a rendszerben jelenlévő felhasználók összekapcsolhatatlanságával foglalkozik, vagyis hogy megállapítható-e, mely felhasználók kommunikálnak egymással.

Integritás (sérthetetlenség) biztosítása: az integritás kritériuma arra vonatkozik, hogy egy harmadik fél nem tudja megváltoztatni két fél kommunikációjának tartalmát.

Megfigyelhetetlenség biztosítása: a megfigyelhetetlenség kritériuma vonatkozik arra, hogy egy harmadik fél nem képes megismerni két fél kommunikációját.

Visszakövethetetlenség biztosítása: a visszakövethetetlenség kritériuma foglalkozik a felhasználói kommunikáció forrásának kiderítéséről. Cél az, hogy egy adott szereplő ne tudja megállapítani, hogy ki adta fel az adott üzenetet.

1. táblázat: A vizsgált attribútumok áttekintése

Általános attribútumok	levél attribútumai	titkosított	cím, fejrész, törzs, csatolmány
		digitálisan aláírt	RSA
		tartalom szerint (csak szöveg, csatolmány, URL)	
Hálózati attribútumok	csatornatitkosítás		SSL, TLS
	támogatott protokollok szerint		POP3, IMAP, SMTP, HTTP, HTTPS
Adatvédelmi attribútumok	anonimitás		anonim remailer-ek, Mixminion
	pszeudonimitás		alfanumerikus karaktersorozat
	összekapcsolhatatlanság		
	integritás (sérthetetlenség)		digitális aláírással
	megfigyelhetetlenség		Mixminion
	visszakövethetetlenség		Mixminion és titkosítás
Biztonsági attribútumok	titkosítás	allokáció szerint	kliens, szerver
		módszerek szerint	public key, SSL, PGP
	a levél védendő részei	cím, fejrész, törzs, csatolmány	
	malware, spyware, vírusok ellen	allokáció szerint	kliens, szerver
		eszközök szerint	programokkal, tűzfalakkal, szűrőkkel
	spam-ek elleni védelem	allokáció szerint	kliens, szerver
		eszközök szerint	programokkal, tűzfalakkal, listákkal
	adathalászat elleni védelem		programokkal, listákkal

7.2. Szolgáltatástípusok (származtatott attribútumok)

Anonim remailer: névtelenséget biztosító e-mail küldő rendszer. Alapvető szolgáltatása, hogy elrejti a kliens személyes információit és anonimitást biztosít számára. Mivel a feladó anonim, teljesül az összekapcsolhatatlanság kritériuma is, hiszen ha a címzett meg is figyelhető, a feladó személye nem kapcsolható hozzá. Az integritás sérülhet, hiszen ha egy harmadik fél a két szereplő között helyezkedik el, és az üzenet nincs titkosítva, akkor anonim módon továbbküldheti azt a címzettnek, miután megváltoztatta az üzenet tartalmát. A megfigyelhetetlenség kritériuma szintén teljesül, hiszen egy támadó nem tudhatja, hogy ki volt egy adott üzenet feladója. A visszakövethetetlenség akkor teljesülhet, ha a feladó egy mix-hálózaton keresztül továbbítja üzeneteit.

Időzített titkosító: ez a megoldás a levelek titkosítását és visszafejtését valósítja meg, azonban oly módon, hogy egy adott idő letelte után ne lehessen dekódolni az üzenetet. Ezt nevezzük „Timed Bomb" funkciónak. Így ha egy üzenet rosszindulatú szereplőhöz kerül, akkor annak nagy valószínűséggel nem sikerül megfejtenie azt az időzítő lejárta előtt, így védve annak integritását [16].

Védelem titkosítással, mix-hálózaton keresztül: ha nyilvános kulcsú titkosítást használunk, és az üzeneteket mix-hálózaton keresztül küldjük, akkor teljesül az integritásvédelem, a visszakövethetetlenség, a megfigyelhetetlenség. Ha duplex kommunikációt tételezünk fel, akkor az anonimitás nem teljesülhet, hiszen a címzettnek tudnia kell, hogy kinek küldje a válaszüzenetet és azt melyik kulccsal titkosítsa, de ehhez elegendő egy pszeudonim azonosító is. Harmadik fél nem ismerheti meg a kommunikáció tartalmát a titkosítás miatt, és nem tudja megállapítani, hogy pontosan honnan küldhették az üzenetet a mix-ek használatából kifolyólag.

Integritásvédelem hitelesítéssel: a hitelesség biztosítása digitális aláírással és titkosítással (rejtjelezéssel) egyszerű, transzparens és könnyen elérhető. A digitális aláírással biztosíthatjuk hitelességünket és az üzenet integritását a címzett felé. Léteznek olyan levelezőkliensek, melyekre plug-in jelleggel telepíthető egy token-alapú titkosító, valamint digitális aláírás készítő. A modul működése automatikus, mindössze két kulcsot kell megadnunk, valamint azt, hogy meddig kívánjuk használni őket. Az egyik a titkosításért, a másik a digitális aláírásért felelős. A címzett a fogadó oldalon ugyanúgy kapja meg az üzenetet, de biztos lehet annak sértetlenségében.

8. Egymásnak ellentmondó tulajdonságok vizsgálata

Az alábbi tulajdonságok ellentmondásba kerülhetnek egymással a definícióik alapján.

8.1. Anonimitás és hitelesség

Egy rendszerben nem lehetünk egyszerre névtelenek és hitelesek is, hiszen a hitelesség kritériuma magában foglalja azt, hogy megbízható módon képesek vagyunk igazolni személyazonosságunkat.[11] Ehhez ugyanis vagy hiteles e-mail címet kellene használnunk, tehát személyhez köthetőt, amelyet más nem használ, de ekkor sérülne az anonimitás kritériuma. A másik lehetőség, hogy engedünk az anonimitás kötöttségéből, csak pszeudonimitást tételezünk fel, és nyilvános kulcsú infrastruktúrát használunk. Ekkor minden felhasználónak rendelkeznie kell egy nyílt és egy titkos kulcspárral, ahol a publikus kulcsot használhatja a többi résztvevő, ha egy adott felhasználónak üzenetet akar küldeni. Ám ekkor a küldő személye a címzett számára nem egyértelműen azonosítható, hiszen bárki használhatja az ő publikus kulcsát. Továbbá ilyenkor nyilvánosan elérhető kulcstárakra van szükség, melyeket megfelelő módon védeni kell, például, hogy ne lehessen a kulcsokat kicserélni, manipulálni, és a rendszernek figyelnie kellene, hogy mindenki csak a saját pszeudonim azonosítóját használhassa üzenetküldéskor a feladó mezőben. Ennek a megfordítása lenne a digitális aláírás alkalmazása pszeudonim azonosítókkal, de itt is a kulcstárolásokkal és kulcsmanipulációval kapcsolatos problémák jelennek meg.

8.2. Hitelesség és visszakövethetetlenség

Ha a hitelesség biztosításához a forrás pontos megállapítása szükséges, akkor ellentmondásra juthatunk, hiszen a visszakövethetetlenség magában foglalja azt, hogy a forrást, az üzenet feladóját ne lehessen egyértelműen azonosítani. Ez alól kivétel, ha a felek előzőleg megállapodtak egy közös szimmetrikus kulcsban, amelyet csak az egymás közötti kommunikációban használnak. Ilyenkor, ha a feladó egy mix-hálózaton keresztül küldi el az üzenetét, titkosítva a közös kulccsal, akkor az üzenet a hálózat szempontjából visszakövethetetlen, ugyanakkor hiteles a címzett számára, hiszen csak a feladó és a címzett ismeri a szimmetrikus kulcsot. Feltételezzük, hogy a kulcs nem kompromittálódott.

[11] Vannak azonban olyan megoldások is, például az úgynevezett vak aláíráson alapuló protokollok alkalmazása, amelyekben a résztvevők egy része úgy fogadja el az adott tranzakciót hitelesnek, hogy a tranzakcióban résztvevők kilétét nem ismeri. (Lásd például Székely I.: Hitelesítés azonosítás nélkül? A privacy technology. *Magyar Távközlés,* Vol. V., No. 11., Budapest 1994.) – *A szerk.*

9. Zárszó

A felhasználó szempontjából számos lehetőség nyílik a biztonságos levelezés megvalósítására. Az ideális levelezőkliensnek a fenti tulajdonságokból minél többet kell tartalmaznia. A legfontosabb a megfelelő biztonság nyújtása mellett az, hogy a segédeszközként használt alkalmazás minél egyszerűbben kezelhető legyen, így az átlagos felhasználók is könnyen boldogulhassanak vele. A legtöbb alkalmazás hátránya, hogy nem ingyenesen hozzáférhető program, valamint a kezelése nem teljesen transzparens. Remélhetőleg a jövőben egyre több levelező alkalmazásba lesz beépítve a tanulmányban szereplő adatvédelmi és biztonsági kritériumoknak megfelelő modul, amelyekkel sikeresen óvhatjuk levelezésünket és adatainkat az illetéktelenekkel szemben.

Hivatkozások

[1] Levelezési statisztika a T-online oldaláról
http://www.t-online.hu/ajanlataink/termekek/20070212freemail.html

[2] CNW Rendszerintegráció honlapja, levelezési termékek bemutatása
http://www.cnw.hu/cnwportal/index.nsf/v_data_by_id/AID71U66U69U84U54U72U51U66U76U77U?OpenDocument

[3] Origo Freemail felhasználási feltételek
http://origo.hu/freemailcikk/20070319felhasznalasi.html

[4] Pettkó András honlapja az internetes cenzúráról
http://www.pettkoandras.hu/01-tarsadalmi_biz-kibont.php?id=4372

[5] GTS Datanet Általános Szerződési Feltételek
http://datanet.hu/05uszi/aszf.html

[6] Adatvédelmi biztos honlapja
http://abiweb.obh.hu/abi/index.php

[7] A Yahoo és a Microsoft szerepe a kínai cenzúrában
http://www.sg.hu/cikkek/54521/a_yahoo_es_a_microsoft_is_segiti_a_kinai_cenzurat

[8] SpamWiki
http://hu.spam.wikia.com

[9] A PET Portál és Blog a magyar közösségi oldalakon megjelenő spam-ekről
http://pet-portal.eu/blog/2007_05_20_Ellenallhatatlan_kozossegi_direkt_marketing/

[10] Egyéni oktatás, áttekintés a számítógépes vírusokról
http://www.egyenioktatas.info.hu/blog

[11] Gulyás Gábor György: Anonim-e az anonim böngésző? Technológiák és szolgáltatások elemzése. In: *Tanulmányok az információ- és tudásfolyamatokról 10.* Alma Mater sorozat, BME GTK ITM, Budapest, 2006 március.

[12] Bencsáth Boldizsár: A hálózati vírusvédelem és a szolgáltatásmegtagadásos támadások elleni védekezés problémái és kapcsolatai, BME HIT, 2004
https://nws.niif.hu/ncd2004/docs/phu/026.pdf

[13] George Danezis, Roger Dingledine, Nick Mathewson: Mixminion: Design of a Type III anonymous remailer protocol, Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 2003, pages 2–15
http://mixminion.net/minion-design.pdf

[14] Egy konkrét mixminion implementáció, [ANN] Mixminion 0.0.8alpha3
http://archives.seul.org/mixminion/dev/Sep-2007/msg00025.html

[15] Internet Szolgáltatók Tanácsa
http://www.iszt.hu/iszt/aup.html

[16] CenturionMail
http://www.centurionsoft.com