Az internetes vírus- és spamvédelem rendszerszemléletben

Bencsáth Boldizsár

BME Híradástechnikai Tanszék
bencsath@crysys.hu

Az elmúlt időszak bebizonyította, hogy a régóta ismert vírusok és kéretlen reklámlevelek olyan súlyos problémát jelentenek az Internet szereplőinek, amit nem lehet figyelmen kívül hagyni.
A cégek többsége jelenleg is használ vírusvédelmi és kéretlen levelek szűrésére alkalmas eszközöket.
A vírusok és férgek ennek ellenére gyakorta megelőzik, kicselezik a védelmet és bejutnak a cégek hálózatába. A kéretlen levelek elleni védelem pedig gyakorta hibázik és kiforratlannak tekinthető.

A vírusvédelem formái

A vírusok elleni védekezés alapjaiban véve a klienseknél kezdődött, főként víruskereső és –irtó szoftverek megjelenésével. A keresés kezdetben esetleges volta később automatizált, folyamatos vírusvédelemmé alakult a kliens oldalon. A vírusok és még inkább férgek által kihasznált programhibák ellen a védekezés a szoftverek és a rendszer frissen tartásával és annak megfelelő ellenőrzésével érhető el, ami már túlmutat a vírusvédelmen. Ha a frissítés nem valósítható meg, úgy a tűzfalas védekezés jelent további védelmi lehetőséget az ilyen támadások ellen.

A kliens oldali védelem legnagyobb problémája a mai napig az, hogy nincsen, vagy rosszul működik: A védelmi szoftverek pénzbe kerülnek, amit még mindig nem mindenki fizet meg, vagy ha meg is fizet, akkor sem tudja megfelelő frissességben tartani a védelmi rendszerét, amely így hatástalan lesz.

A vírusok jelenlegi legnagyobb veszélye nem az a károkozás, amelyet az egyedi kliensekre jelentenek. Nem az jelenti ma a legnagyobb veszélyt, hogy egy vírus le fogja

törölni a merevlemez teljes tartalmát. A veszély jelenleg inkább abban áll, hogy a cég titkos információi napvilágra jutnak, a cég napokig nem tud működni, hogy a cég vagy akár az ország számítógépes hálózata lelassul, működésképtelen lesz, vagy nehezíti a munkát, csökkenti a teljesítményt. További veszélyeket rejt a globalizáció: Az Internet a számítógépeket olyan rendszerbe szervezte, amely az egyes gépeken elhelyezkedő vírusokat hangyákhoz teszi hasonlóvá. A hangyák egyesével kevéssé veszélyesek, de a sok megtámadott, megfertőzött számítógép együtt komoly veszélyt jelent.

A veszély tehát jelentős, érdemes megerősíteni a védelmet. A megerősítés, és egyszerűsítés elve mentén haladva jelentek meg a központosított megoldások: Egy szervezet minden munkaállomására víruskeresőt telepítünk, amelyek a cég központi szerverével állnak kapcsolatban. A központi szerver ismerheti a kliensek állapotát, és ellenőrzött módon hajthatja végre a kliensek vírusadatbázisainak frissítését. Ezt tekinthetjük a rendszerszemlélet egyik megjelentésének a mai vírusvédelmi rendszerekben.

Természetesen a klienseken túl a fájlszerverek is védelemre szorulnak, így a víruskereső programok többsége megjelent a fájl szerverekre szánt különleges verzióban is.

A megoldás használata során felmerülhet a kérdés: Ha az internetes levelezés lett a vírusok bekerülésének legfontosabb közege, miért nem kapcsolunk az internetes levelezésre is vírusvédelmi szoftvert. Nos a kérdést tett követte és még ma is egyre-másra jelennek meg az e-mail szervereket védő szoftverek.

Sokak tévesen úgy gondolják ma is, hogy ha a vírusok e-maileken jönnek, és az e-mail rendszert megfelelő szoftver védi, akkor a kliens oldali védekezés elhanyagolható, felesleges. Számos példa mutatja azonban, hogy ez koránt sincs így. A vírusok gyorsabban terjedhetnek el, mint amilyen gyors a vírusvédelmi szoftverek frissítése. Ilyen esetben elképzelhető, hogy egy vírus védelmi rendszerünk frissítése előtt eljut valamely munkaállomásunkra. Amennyiben a védelem a munkaállomásra is kiterjed és megfelelően van beállítva, úgy a megfelelő frissítés letöltése után a fertőzött munkaállomás gyorsan felismerhető, illetve a fertőzés akár a szoftver automatikus működésével is megszüntethető. Ha azonban a bejutott vírus korlátlanul működhet belső hálózatunkon, úgy könnyen átterjedhet a gond a többi munkaállomásra is, és innentől a helyreállás hosszú időt és sok munkát igényel.

Elmondhatjuk tehát, hogy a vírusok elleni védekezés egy cég belső hálózatán több helyen szükségesen megvalósítandó feladat.

A vírusvédelmi rendszerek az elmúlt években a fenti környezeti változások hatására megváltoztak: A cégek egyre-másra hozták ki a komplex megoldásokat, amelyekkel a levelezési rendszer is védhető. Ezek a megoldások egyszerre számos dolgot kívánnak megvalósítani komplex rendszerben: A levél fogadását, a fejléc feldolgozását, a csatolt fájlok kikódolását és kitömörítését, a vírusok és ártalmas kódok, esetleg kéretlen adatok felderítését, majd a levél továbbítását, várakoztatását, elutasítását, stb.

Ezt a fajta komplex szemléletmódot tekinthetjük ma a rendszerszemlélet második fontos megnyilvánulásának a vírusvédelemben.

Komponens alapú védekezés

A vírusvédelem során a fentiekben láthatóan igen sok különböző feladatot kell megoldani, kezelni, főleg ha e-mail vagy más hálózati kiszolgálókról van szó.
A gyártók többsége ezeket komplex módon, egyetlen termékkel kívánja lefedni. Ez a megoldás valóban célszerűnek tűnhet, hiszen a boltban megveszünk egy terméket és az minden problémánkat megoldja. A gondot azonban ezzel csak részben oldjuk meg. A cégek többségében, a védett hálózatokon számos olyan probléma jelentkezhet, amely egyedi, vagy egyedileg beállított megoldást igényel.
Rövidlátásra vall továbbá az is, ha úgy gondoljuk, hogy a vírusvédelemnek csak a mi rendszerünket kell megvédenie. Ez nem igaz: A rendszernek meg kell védenie az Internet többi részét is saját számítógépeinktől, valamint komplex rendszert kell képeznie annak érdekében, hogy az új, ismeretlen vírusok elleni védekezés is hatékony legyen.

A Unix alapú, ingyenes, vagy olcsó megoldások általában komponens alapon jöttek létre a Unix világ KISS (keep it simple, stupid) felfogását követve. A komponenseket a szükségleteknek megfelelően fejlesztették ki, majd kapcsolták össze.

A levél kézbesítési folyamata alapvetően a következő szakaszokra bomlik:

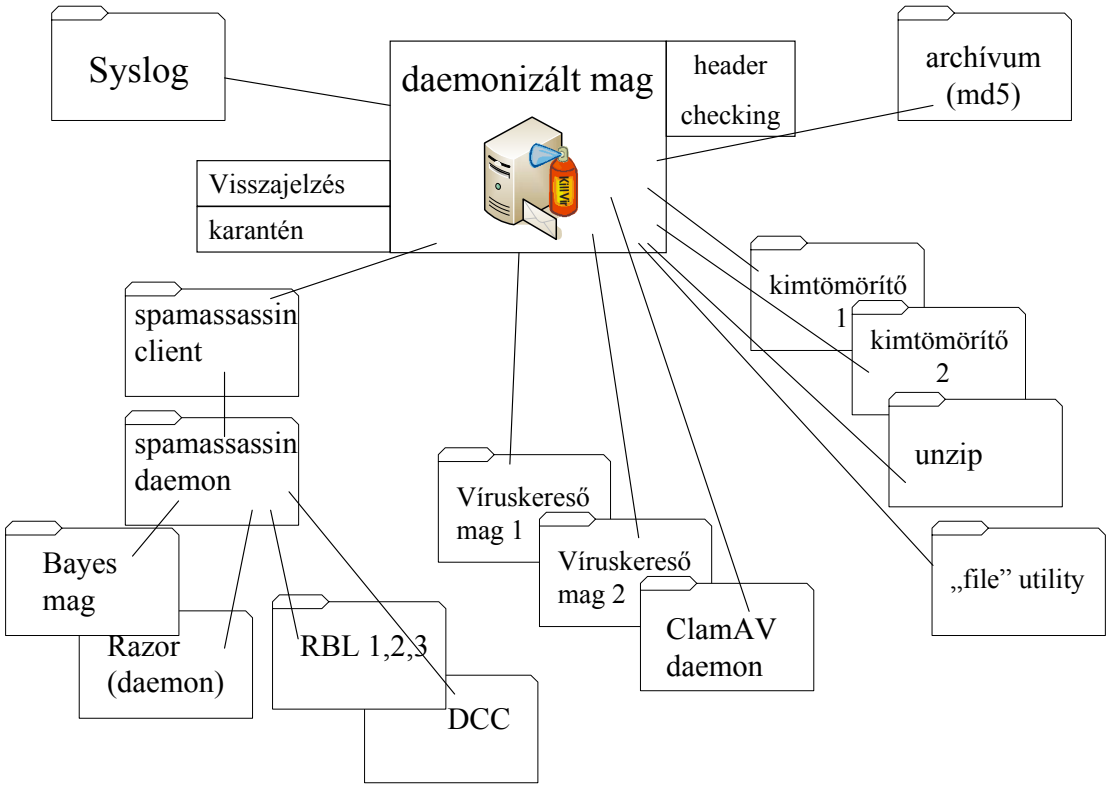
- A levél átvétele a szomszédos SMTP szervertől (MTA- Mail Transport Agent funkció)
- A levél átvizsgálása vírusok és/vagy spam szempontjából
- A levél kézbesítése lokálisan, vagy továbbküldése

A levél helyi kézbesítésekor természetesen gyakorta lehetőség van még további szűrők használatára is, ilyen megoldás lehet, amikor a levél helyi kézbesítését a *procmail* szoftver végzi, és az egyes felhasználók egyedi módon kiszűrik a spam vagy vírus gyanús küldeményeket.

A fenti példánál maradva a levél átvizsgálához is számos funkció társul:

- A levél fejlécének analízise
- Levél fejléce alapján spam ellenőrzés pl. RBL szűrőlisták segítségével
- A levél kicsomagolása, a MIME komponensek kibontása, esetleges tömörített fájltartalmak kibontása
- Az egyes fájlok, tartalmak egyedi átvizsgálása vírusvédelmi szempontból (akár több különböző vírusirtó segítségével)
- Vírus észlelése esetén riasztás küldése a megfelelő személynek, esetleges értesítés a küldő és/vagy fogadó felé a vírus észleléséről, a vírusos küldemény tárolása
- Levél tartalma alapján heurisztikus és egyéb spam szűrési vizsgálatok

A fenti feladatok mindegyikére külön-külön fejlesztett komponensek léteznek, ezeket egyes központi magok fogják össze. Példaként: Az SMTP protokoll feladatait ellátó komponens alapú rendszert (pl. postfix) egészíti ki egy másik komponens alapú rendszer, amely egy vírusvédelmi magra (pl. amavisd) épül, ez használja ki a különböző további szolgáltatások lehetőségeit.
A felhasznált komponensek sokaságáról az 1. ábra tartalmaz bevezető jellegű áttekintést.



1. Ábra. Amavisd magra épülő ellenőrzési rendszer komponensei

A rendszerszemélet fontossága

Nem azért fontos a komponens alapú szemléletmód, mert így egy gép védelme lényegesen hatékonyabb lehet. Amennyiben egyetlen gyártó egyetlen integrált terméke minden feladatot tökéletesen megoldana, nem volna szükség rendszerkomponensekre. A UNIX világban megfigyelhető tapasztalat azonban az, hogy a legegyszerűbb komponenseket is évek, évtizedek óta fejlesztik, javítják. Ha évek, évtizedek alatt nem sikerült minden hibát kigyomlálni egy egyszerű szoftverrészből, akkor kevéssé elképzelhető az, hogy egy kereskedelmi szoftvereket gyártó cég néhány év alatt egymagában olyan szoftvert képes gyártani, amely nemcsak szolgáltatásaiban és színvonalában kerül az élmezőnybe, de hibalehetőségeket is csak kevéssé tartalmaz.
Sokkal célravezetőbb lehet tehát komponensekből összeépíteni egy rendszert, mégpedig olyan komponensekből, amelyeket egyedileg jó minőségben, ellenőrzött módon készítenek el, és az összehangolás is komoly kontroll alatt van.
Ez azonban jelenleg idegen a kereskedelmi szoftverek világától. Az üzleti logika ugyanis azt diktálja, hogy komplett megoldásra alkalmas szoftvert kell eladni, és nem olyat, amelynek részeire a kezelőnek rálátása lenne. Viszont ez látszatmegoldás, és leginkább a vitatott „security by obscurity” elvre hasonlítható.

A legfontosabb haszna a komponens alapú (rendszerszemléletű) struktúráknak a kiegészíthetőség. Ha egy újabb komponenst építünk a rendszerbe, az gyakorta az előző komponensek minimális megváltoztatásával, vagy a rendszer kis mértékű átkonfigurálásával megtehető. Az új komponensek pedig újfajta lehetőségeket nyújtanak, és jelenleg ennek kiemelkedő fontossága van: Az e-mail vírusok, spyware-ek, kéretlen reklámlevelek nem változtak meg igazán számottevően a néhány évvel ezelőtti állapotokhoz képest. Az azonban megváltozott, hogy a fenti veszélyek hogyan és milyen károkat okoznak.
A megváltozott károkozás több érdekes problémát vet fel:

- A legnagyobb kár nem annál keletkezik, akit vírusfertőzés ért. A fertőzött számítógépeket „zombi" módjára távirányítással vezérelnek, így azok felhasználhatók kéretlen reklámlevelek tömeges kiküldésére, vagy pl. DoS (szolgáltatásmegtagadásos támadás) véghezvitelére.
- Hiába védjük cégünket a legújabb szoftverek legfrissebb adatbázisaival, ha azok egy naposak. A 15 perce terjedő vírus már gépek millióit veszélyeztetheti, és ez ellen védtelenek lehetünk.
- Hiába vannak jó védelmi szoftvereink, ezek gyakorta nem segítenek abban, hogy a vírus készítőjét fel lehessen deríteni. (Ennek ellenére ebben az évben minden eddiginél több víruskészítőt sikerült leleplezni, miközben a vírusfertőzések száma is megdöntött minden eddigi statisztikát), elrettentő erőt az jelenthet, ha hatékony, átlátható rendszerek segítenek a terjesztők felderítésében.
- Hiába tudjuk detektálni a vírusokat és visszajelezni a vírusküldő felhasználóknak, ha nem is a levélben szereplő feladó adta fel a vírust. A visszajelzéssel DoS támadást okozhatunk, a visszajelzés hiánya jogi problémákhoz vezethet, a valódi feladó felderítése pedig szinte lehetetlen.
- Hiába tudjuk, hogy mely gépek küldik a vírusokat, ha azokat nem tiltjuk ki, ha azokat közvetlenül, vagy az ISP-jük által nem tudjuk értesíteni.

Javaslatunk a fentiek tükrében a következő: A mai rendszereket úgy kell átalakítani, hogy azok alkalmasak legyenek a megváltozott és folyamatosan változó igények optimalizált kielégítésére. Ez azt jelenti, hogy:

- Ki kell dolgozni hatékony komponenseket az újabb problémák megoldására, mint egyéni védekezési lehetőségek, statisztikai adatgyűjtés, azonosítás, visszajelzés, tesztelés, karanténozás, mindezek távoli adminisztrációja és koordinációja tekintettel a hiányos információs viszonyokra.
- A komponensek támadhatóságát minimalizálni kell egy ráépülő bizalom alapú rendszer alkalmazásával.
- A komponensek működését (pl. DNS RBL listák különböző célokkal) szabványokban (akár de facto, akár formális) kell rögzíteni annak érdekében, hogy az újabb, eltérő vagy azonos célú komponensek a legkönnyebben alkalmazhatóak legyenek.
- A komponensek összeépíthetőségét szabványokkal érdemes leírni, hogy azok a lehető legjobban (legkompatibilisebb módon) össze- illetve bekapcsolhatóak legyenek.
- A kereskedelmi szoftverek se a „mindent belerakni" elvet kövessék, hanem a fenti szabványok szerinti darabolást támogassák.

- Globális (esetenként regionális) rendszereket kell kiépíteni annak érdekében, hogy a vírusveszélyre való reagálás is megfelelő mértékű, koordinált, együttműködő és hatékony legyen. Ezeknek a rendszereknek a következőket kell támogatnia:
    - új vírusok azonosítása
    - vírusfertőzés terjedésének diagnosztizálása, segítése, az aktuális állapot felmérése
    - a vírusinformációk hatékony elosztása
    - a vírusvédelmi rendszerek hatékony (önkéntes alapú) tesztelése
    - a fertőző gépek azonosítása, adatbázis a veszélyes forrásokról
    - ISP-k közötti adatcsere globális támogatása a fertőző gépek kiiktatása céljából
    - globális karanténozási logika
    - megbízhatóság globális kezelése

Mitől lesz a vírusvédelem tehát igazán rendszerbe szervezve?

- Az egyedi, számítógépre telepített védelmi szoftver komponensek tucatjából építkezik, ezek vannak jól összehangolva.
- A komponensek cserélhetőek, kiegészíthetőek, egyedileg frissíthetőek.
- Az egyedi számítógépet megfelelő karbantartók távolról is adminisztrálhatják pl. céges hálózatban. Az adminisztrációs során a védelem kiegészíthető lehet újabb komponensekkel.
- A komponensek hatékonysága mérhető, így a rendszer optimalizálható
- Egyes komponenseket regionális, országos vagy globális rendszerekbe lehet és kell szervezni, ilyen pl. a statiszikai adatgyűjtés. (pl. hollandiai vírusos gépeket nyilvántartó adatbázis)
- A nagyméretű szervezett rendszerek központjai nem feltétlenül kereskedelmi cégek, hanem olyan szervezetek (non-profit, kormányzati, vagy kereskedelmi), melyek megbízhatók, az adatokra épülve megfelelő döntést, vagy döntéselőkészítő összegzést tudnak adni, és ezt nyilvánosan kezelik. (Ilyen részben néhány honeypot kapcsolatos projekt (honeynet stb.))
- A megbízhatóság kiemelt fontossága miatt ilyen központ természetesen több is létezhet, egy komponens akár több központtal is kapcsolatot tarthat. (Ez igaz ma pl. az RBL-ek esetén)

A fentiek segítségével olyan rendszerek jöhetnek létre. amely egy-egy megoldást világméretű együttműködő rendszerré tudnak fejleszteni. Ezek között a rendszerek között is megfelelő koordináció, szervezettség valósítható meg amellett, hogy a rendszerek önállósága megmarad. Az ilyen jól koordinált, de elosztott, világméretű, de skálázott rendszer már valóban hatékony lehet az Internetes károkozók ellen.
Nem mondhatjuk, hogy mindez újdonság volna: Főleg az ingyenes megoldások körében, de ma is megfigyelhetőek azok az önszerveződő megoldások, amelyek ilyen jól koordinált, de önkéntes, önálló rendszereket hoznak létre. A spam-védelmi rendszerek többsége ma is több részmegoldás alapján, heurisztikát alkalmazva dönt a levelek sorsáról. Az is megfigyelhető azonban, hogy a kereskedelmi termékek általában kevéssé

vesznek részt ezek kialakításában, használatában, elterjesztésében, továbbá a hatékony működést támogatná a megfelelő jogi keretek létrejötte is. (Érdekes módon a spam védelem esetében a kereskedelmi termékek is jobban elfogadták a komponens-szemléletet) További fontos szempont az elterjedtség kérdése: Az ilyen rendszerek jelentős része csak megfelelő méretű elterjedtség esetén lehet hatékony, ezért kezdetben érdemes lehet kisebb méretben (országos szinten, akár pl. ISP-k összefogása mellett) bevezetni azokat.

Megoldások

A fenti problémákról részletekbe menően hosszú oldalakat lehetne írni, ám jelen írásban csak néhány problémát emelünk ki. A kiemelt problémákkal kapcsolatosan saját magunk végzünk kisebb-nagyobb kísérleti fejlesztéseket és kutatásokat.

Vírusforrás azonosítása csapda e-mail cím segítségével

A vírusok elleni küzdelem kiemelt pontja az általános internetes biztonsági szint emelése. Sajnálatos módon az Internet növekedése azt vonta maga után, hogy a kevéssé adminisztrált, kevéssé ellenőrzött gépek száma arányaiban és abszolút mértékben is megnőtt.
Az internetes vírusok többsége ma már hamisítja a feladót, és így küldi tovább a fertőző kódot. Fontos feladat tehát a vírusforrások azonosítása. Az ISP-ken keresztül, törvényi kötelezettség, lehetőség, és megfelelő hajlandóság esetén a tulajdonos-fenntartó értesítése megtehető, de kevéssé hatékony. Jelenleg nincsen szabványosítva az adatcsere a szolgáltatók között, így a fertőző számítógépekről szóló információk továbbküldése és feldolgozása esetleges.
A vírusok többsége a hamisított feladó címeket, és a célszemélyek címét a fertőzött számítógépekről szerzi: átnézi a fájlokat és összegyűjti a címeket. A fertőzések emiatt követik a tulajdonosok szociális rendszerét, általában ismerősök, barátok felé terjednek tovább a leghamarabb. Ezt kihasználva rendszerünk hamis, csapda e-mail címekre épül: Az e-mail címeket a felhasználó számítógépén helyezzük el megfelelő fájlban és/vagy a felhasználó „címlistájában". Amennyiben a felhasználó számítógépe megfertőződik, úgy az egyedileg generált csapda e-mail cím a címezettek, vagy a feladók között felhasználásra kerülhet. Ha pedig egy védettebb gép ezt felismeri (pl. visszajelzést küld „vírusos levél küldéséről", úgy az egyedileg kiadott csapda cím alapján a vírusfertőzött gépet a rendszer azonosítani tudja. A fenti megoldást a magyar OpenOffice.Org ingyenes irodai programcsomag szoftverregisztrációs rendszerébe integráltuk. ([5])

VIRUSFLAGS projekt

Az e-mail alapú vírusok gyakorta hamisítják a feladót. Ebben az esetben vírusos levél fogadása esetén balgaság lenne „vírusriasztást" küldeni a hamisított feladónak, mert ez csak félrevezető lehet. Ellenben ha a vírus (pl. word makróvírus) nem hamisítja a feladót,

és gépünk a levelet kitörli, ám a küldőt nem figyelmezteti, úgy jogi problémák adódhatnak: Ha cégünk egy szerződés felmondását nem fogadja be, mert makróvírussal fertőzött, de figyelmezetést sem nyújt, az jogi problémát jelenthet.
A VIRUSFLAGS projekt keretében olyan komponens létrehozásán fáradozunk, amely alkalmas a fenti probléma hatékony megoldására. A megoldás alapja az, hogy az adott vírusról meg kell tudnunk azt, hogy a vírus hamisítja-e az e-mail címet vagy sem. A víruskeresők ezt az információt maguk is tudhatják, ám rendszer- vagy komponensszemlélet figyelembe vételével ennél hatékonyabb lehet az, ha egy rendszerkomponens csak azzal törődik, hogy válaszolni tudjon arra a kérdésre, hogy a vírus hamisítja-e a feladót, vagy sem.
A kiépítendő rendszerünk a DNS RBL rendszerekhez hasonlóan kérdezhető le. A megkapott információ alapján meg tudja válaszolni azt a kérdést, hogy a vírus hamisítja-e a feladó címét vagy sem. A hamisításra hajlamos vírus esetén nem kell visszajelzést küldeni, míg a nem hamistó vírusnál igen. A projekt ennél általánosabb célt próbál elérni: A vírusok fontos tulajdonságai legyenek lekérdezhetőek központilag, méghozzá úgy, hogy ezek az információk megbízhatóak legyenek.
Kiegészítésként a VIRUSFLAGS rendszer jelenlegi szoftverkomponensei alkalmasak arra is, hogy statisztikai adatgyűjtést végezzenek a különböző vírusok terjedéséről.

SPAM jogi koordináció

A VIRUSFLAGS projekt kivitelezése kapcsán merült fel az az igény, hogy magyar viszonyok között alkalmazható hatékony koordinációs lehetőséget készítsünk a kéretlen reklámlevelek küldői ellen. A kéretlen reklámleveleket a hazai viszonyok között valódi, nem hamisított feladóval adják fel, de törvényt sértő módon, ami ellen jogi eljárás kezdeményezhető. A cégek többsége azonban nem is tudja, ha valaki neki törvénytelen módon küld reklámlevelet. A VIRUSFLAGS rendszer koordinációs komponense lekérdezheti valamely szervert, hogy az adott levél küldője szerepel-e a magyar kérelten reklámlevél küldők listáján. Amennyiben a feladó feltehetően kéretlen reklámlevelek ismert küldője, úgy a levél (a fogadó előzetes felhatalmazása szerint) továbbküldhető egy központi koordinációs szervezetnek. Ez a szervezet (legyen az kereskedelmi cég, a felhasználó Internet-szolgáltatója, vagy kormányzati szerv) az összegyűjtött nagyszámú levél alapján tömeges (nagyszámú egyedi vagy gyűjtő jellegű), koordinált, központosított jogi eljárást tud kezdeményezni a levelek küldője ellen.

DDoS támadások

A szolgáltatás-megtagadásos támadások (Denial-of-Service, DoS) kiemelt jelentőséggel bírnak az Internet biztonsági problémái között. A DoS támadások során a támadó célja nem az, hogy a hálózatba behatoljon, kizárólag az, hogy megakadályozza annak megfelelő, üzemszerű működését. Ennek következtében a támadó eszköztára igen tág,

míg a védekezés eszköztára kicsi. Gyakran a hálózat biztonsági alrendszerei maguk teszik a hálózatot veszélyeztetetté DoS támadásokra.

A DoS támadások általános esetben elosztott támadások, ahol több támadó együttes cselekedettel kívánja előidézni a rendszer összeomlását. Ezt Distributive DoS támadásnak, azaz DDoS-nek hívjuk. A DDoS extrém esete az, amikor csak egyetlen állomásról indítanak támadást (DoS).

A DoS típusai

Protokoll hiba

A DoS támadások egyszerű változata az, amikor valamelyik protokoll vagy szoftver hibáját egy rosszindulatú támadó arra tudja felhasználni, hogy az adott szolgáltatást, vagy szervert működésképtelenné tegye. Ilyen közismert támadás volt a ping-of-death, amikor egy megfelelően formázott IP csomaggal „lefagyaszthatóvá" váltak egyes számítógépek.
A hibás szoftverekből, protokollokból adódó problémák egyszerű javítása a hiba korrigálása, hosszútávon a szoftverek frissességének és hibajavításának koordinált, jól szervezett telepítése és fenntartása.
Ennek megfelelően a protokoll hibák esetében egyrészt megoldható a hiba megszüntetése kijavítással, továbbá az ismeretlen hibák elleni védekezés is támogatható különböző módokon. (pl. tűzfal, nem használt szolgáltatások letiltása, heterogén több kiszolgálós környezet felépítése stb.).

Hálózati elárasztás

A DoS támadások veszélyes esete a hálózati elárasztás. Ilyen esetben többnyire nagyszámú kliens egyszerre kezd forgalmazni nagy adatmennyiségeket egy vagy több szerver irányába: a nagyszámú kliens összforgalma olyan magas lehet, hogy azt a szerver hálózati kapcsolatai és esetleg erőforrásai sem bírják kiszolgálni.
Az ilyen hibák ellen védekezni a megtámadott gépnél többnyire igen nehéz.

- Amennyiben az elárasztó forgalmat nem tudjuk különválasztani a legitim forgalomtól, úgy a forgalom kitiltása csak úgy lehetséges, ha a legitim felhasználók forgalmát is kitiltjuk, és ezzel már önmagában megvalósul a szolgáltatás-megtagadás célja.
- Amennyiben az erőforrásaink növelésével kívánunk védekezni, úgy a támadó is növelheti erőforrásait, a támadás méretét több támadó bekapcsolásával.
- Amennyiben sikerül azonosítani a támadó forgalmat és különválasztani azt a legitim forgalomtól (pl. forgalomstatiszikai alapon, azonosítással, vagy a lekérdezések kategorizálásával) úgy a felesleges forgalom kiszűrhető. 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.

([4]) Ennek megfelelően az ilyen jellegű védekezés igen nehéz, vagy akár lehetetlen akkor, ha a védelmet csak a fogadó fél oldalán kívánjuk kiépíteni.

Szerver túlterhelés

A hálózati elárasztás többnyire buta módon megpróbál felemészteni minden hálózati kapacitást. A támadó kihasználja nagy számú kontrollált állomásából adódó óriási kapacitását és így éri el a célját. Sokkal kifinomultabb módszer azonban az, ha a hálózati protokollokban, szolgáltatásokban olyan elemet sikerül találni, amelynél a kérdező fél (kliens) viszonylag kis ráfordítással (számítási, hálózati kapacitással) el tudja érni, hogy a kiszolgáló nagy ráfordítással válaszoljon a kérésre.
Ilyen lehet az, ha egy kiszolgáló egy kis kérésre hosszú adatmennyiséggel válaszol, vagy az, ha egy rövid kérés kiszolgálása hosszú számítást követel meg a szerver oldalán. Egy rosszul kivitelezett adatbázis alapú weblap esetén elképzelhető például, hogy egy kérés kiszolgálása az adatbázisban olyan, rosszul indexelt, nagy adatmennyiséget feldolgozó feladatokat indít el, amely kiszolgálás erőforrás-felhasználása jóval meghaladja a kérés igényeit.

Az ilyen támadások esetében a támadó legitim, kis adatforgalom mellett is meg tudja bénítani a szervert. A védekezés természetesen elképzelhető, ha tudjuk mérni, mely kérések veszélyesek, és meg tudjuk automatikusan vizsgálni, hogy valaki direkt ilyen kérésekkel fordul-e hozzánk. Kétséges azonban, hogy pusztán a kérés analízisével megkülönböztethető a támadó és egy legitim felhasználó, valamint az, hogy ennek segítségével úgy sikerül megvédenünk a szervert, hogy legitim felhasználót nem veszélyeztetünk.

Legutóbbi támadások

A legutóbbi évek DoS támadásai a legtöbb esetben egyszerű elárasztásos támadások voltak. Az elárasztás is lehet sokféle, a gyakorlatban felmerült támadások többsége a TCP SYN adatcsomagjait kihasználó támadás, illetve ICMP forgalomra építő támadás. Mindkét támadási formánál mód van a feladó IP címének hamisítására is, míg például a túlterheléses támadásoknál ez ritkábban fordul elő, a feladó IP címének hamisítása pedig segíti a támadó elrejtését.
Alkalmanként előfordul protokoll hibát kihasználó DoS támadás is, de ezek többnyire rövid ideig tartanak, hiszen a hiba kijavításával a probléma gyorsan megszüntethető.

Számos DoS támadást hajtottak és hajtanak végre folyamatosan a kéretlen reklámlevelek ellen létrejött megoldásokat nyújtó cégek ellen. Ez a folyamat azt sugallja, hogy a kéretlen-reklám-ipar egyre veszélyesebb lehet az Internet számára.

Az utóbbi időszak vírustámadásainál egyre gyakrabban derült ki az is, hogy a vírusba olyan rutint programoztak, amely valamely cég hálózatának DDoS támadással történő lebénítását célozza meg. A Mydoom.A vírus így támadta meg 2004. februárjában az SCO

hálózatát, illetve a vírus átírt, Mydoom.B változata hasonló módon a Microsoft hálózatát. A támadás itt elárasztásos támadást jelent, oly módon koordinálva, hogy az egyes víruspéldányok azonos időpontban kezdik támadni a cég lapját kiszolgáló szervert.

Az SCO elleni támadás látszólag sikeres volt, mivel a cég weblapja elérhetetlenné vált, igaz, többen megkérdőjelezik azt, hogy az SCO nem tudott volna-e védekezni a támadás ellen, valamint megemlítik annak a lehetőségét, hogy az SCO maga tiltotta le weboldalát a támadás kezdetekor. A Microsoft oldala ezzel szemben működőképes maradt, ami jórészt annak köszönhető, hogy a cég weblapját egy igen nagy kapacitással rendelkező tükröző hálózaton keresztül teszi elérhetővé.

A vírusvédelem és a DoS támadások kapcsolata

A vírusvédelem és a DoS támadások több helyen kapcsolódnak egymáshoz. A víruskódba elhelyezett DoS támadást segítő rutin mellett számos más probléma is létezik.

- Amennyiben a vírus éppen járványszerűen kitör, elárasztja a felhasználók postaládáját, akik (amennyiben nem védekeznek a vírusok ellen) a sok levél miatt nehezen találják meg fontos leveleiket vagy betelik postaládájuk.
- A vírusvédelmi eszközök a feladók részére gyakran hibaüzenetet küldenek („az ön által küldött üzenet vírust tartalmaz így nem került továbbításra”), amely elárasztja a hamisított feladó postaládáját (lásd dumaru vírus).
- Amennyiben a vírus hamisított feladóval továbbítja magát, ám a címzett hibás, úgy a hamisított feladóhoz nagyszámú kézbesítési hiba visszaigazoló üzenet érkezhet, amely DoS-t eredményezhet.
- Amennyiben valamely levelező szerverre a vírus egyszerre igen sok levelet kézbesít (pl. lassú Internet kapcsolat kifele mutató levelező tűzfalára egy belső fertőződés után), úgy az leterhelheti a hálózati kapcsolatot, továbbá a vírusos levelek víruskeresése a levelező kiszolgáló teljes leterheltségét eredményezheti.

Mit tehetünk az említett problémák ellen?

Egyes problémák ellen gyakorlatilag semmit nem tehetünk: A nevükben hamisított levelek kézbesítési értesítőit szűrhetjük, különválogathatjuk, de más védekezést nem tudunk tenni.
Segítséget jelenthet az egyelőre kísérleti üzemben levő SPF, SenderID (stb.) rendszer bevezetése, ennek használatával elérhető lenne, hogy a nevünkben hamisított levelet feladni ne lehessen, azonban ennek is számos problémája van, így jelenleg még nem jelent megoldást a feladatra.

A víruskereső rendszerektől visszaérkező vírusriasztások által okozott károk viszont csökkenthetőek. A megoldást egyrészt az jelenti, ha a vírusos levelekről nem küldünk riasztást a feladónak. Ilyen esetben természetesen arról sem értesül, ha egy csatolt word

fájlt tartalmazó levele makróvírus miatt nem került továbbításra, így egyes esetekben a riasztás teljes kikapcsolása nem célszerű.
Az Amavis frissebb változataiban például beállíthatóak azok a vírusok, amelyek hamisítják a feladót, és ezen vírusok esetében a rendszer nem küld kézbesítési riasztást. A vírusok listája jelenleg egy reguláris kifejezés, amelynek a vírus nevére kell illeszkednie. Remélhetőleg a probléma később fejlettebb eszközökkel is megoldható lesz.

Vírus-szűrő levelező kiszolgáló elleni támadások

A vírusok által okozott DoS problémák mellett a vírusokkal kapcsolatos másik gond az, hogy maguk a vírusvédelmi rendszerek is érzékenyek lehetnek DoS támadásra.
Ilyen tipikus támadások:

- A vírusvédelmi e-mail átjáró elárasztása vírusos vagy nem vírusos levelekkel;
- A vírusvédelmi átjáró elárasztása olyan formai hibás levelekkel, amely az átjáró működését megbénítja.

Az első típusú támadás esetén a támadó azt használja ki, hogy a vírusvédelmi rendszer nagy erőforrásokat emészt fel. Egy Amavissal, vagy Mailscannerrel felszerelt rendszer kapacitása, főként ha több víruskeresőt is használunk, véges. A kapacitás elérésénél előfordulhat, hogy a rendszer a túlzott kapacitásfelhasználás miatt újraindul (pl. watchdog alapján), vagy a levelek elfogadását a túlterhelés megszűnéséig a rendszer megszünteti. Bárhogyan is történik, a túlterhelés mindenképpen a legitim levelek késését fogja okozni.

A második típusú támadás esetében a protokoll ill. szoftverhiba típusú DoS támadásról beszélhetünk. Ilyenre minták:

- Olyan levél küldése, amely olyan tömörített állományt tartalmaz, amely nagyon hosszú, de igen redundáns (pl. több GB méretű, csak azonos betűből álló fájl). A csatolt fájl mérete így korlátos, azonban a víruskeresés céljára történő kicsomagolás esetén a szerveren a hely elfogyhat, a rendszer megbénulhat.
- Olyan levél küldése, amely sok kis fájlt, vagy további tömörített fájlokat tartalmaz több mélységben, így leterheli mind a kitömörítő, mind az ellenőrző rutinokat.
- Formai hibás fájl küldése, melynek dekódolását végző rutinok a rendszer bénulását eredményezhetik.

A fenti, második típusú problémák a hibák kijavításával, a védelem megerősítésével többnyire kiküszöbölhetőek. Az Amavis programcsomagban például korlátozva van a beágyazott tömörítési szintek száma, továbbá mód van arra is, hogy bizonyos tömörítési arányon túl ne lehessen tömörített fájlt csatolni, így a szabad kapacitást az ellenőrzés már nem fogja felemészteni. Hasonló módon korlátozható a vírusvédelmi rendszer teljesítményszükséglete is: Egy kvóta meghaladása után a védelmi rendszer nem vizsgálja tovább az adott levelet. Természetesen az így kiszűrt levelek a hálózati szabályozásunknak megfelelően kerülhetnek azonnali elutasításra, vagy későbbi vizsgálatok céljára karanténba, stb.

Vírusvédelmi rendszer DoS front-end

Mit tehetünk az ellen a támadás ellen, amikor a rendszerünket legitim levelekkel árasztják el annak céljából, hogy a nagy teljesítményigényű védelmi rendszerünk a szerver túlterhelését okozza?

A kérdés megválaszolása nehéz. Természetesen fokozhatjuk rendszerünk teljesítményét, és megpróbálhatjuk elkülöníteni a támadó szándékú e-maileket a legitim forgalomtól. Elképzelhető azonban, hogy ez nem tehető meg, vagy hogy rendszerünk már viszonylag kevés (néhány tíz, néhány száz) e-mail segítségével megbénítható rövidebb időre, amit el szeretnénk kerülni. A helyzet javítását eredményezheti a levelezés protokoll szintű módosítása client-side puzzle ([2]) technika segítségével. A technika segítségével javítható a teljesítmény-ráfordítás aránya a kiszolgáló és a küldő között, és így megelőzhető a DoS helyzet kialakulása. A technika javítására magunk is javaslatot tettünk ([3]) játékelméleti megközelítés alkalmazása segítségével.

A megoldáshoz az [1] cikkben ismertetett forgalomanalízis módszerét használó elméleti munkánkat kívánjuk bemutatni és javasolni.
A módszer a következő algoritmusokra épít:

- A támadás észlelése
- A támadók elkülönítése a legitim felhasználóktól
- A támadó forgalom kitiltása
- Sikeresség ellenőrzése

Az algoritmus rövid leírása vírusvédelem esetén a következő:

A támadás észlelése

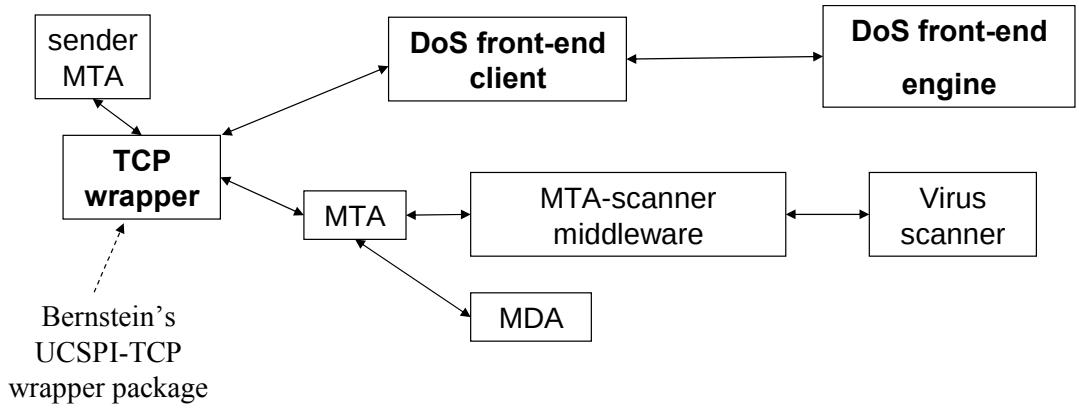
A támadás észlelése a levelezési forgalom folyamatos statiszikai analízisével zajlik. Amennyiben a forgalom hirtelen megnő, úgy a rendszer azt támadásként érzékeli, és innentől kezdve egy korlátozott ideig részletes statisztikát készít, hogy milyen állomások hány üzenetet küldenek.

A támadók elkülönítése a legitim küldőktől

A hosszú távú és rövid távú statisztikai mérések alapján a rendszer megbecsüli, hogy a támadó mekkora forgalmi többletet generál.
A részletes statisztikák alapján a rendszer feladata kiválasztani azokat az állomásokat, akik a legtöbb forgalmat generálják, méghozzá annyi ilyen állomást kell kiválasztani, amelyek összforgalma megegyezik a támadás becsült méretével.

Miért azokat az állomásokat kell kiválasztani, amelyek a legtöbb forgalmat generálják? Ez az algoritmus kulcsa. A támadó, ha DDoS támadást hajt is végre, mindenképpen

megpróbálja a támadó gépek számát minimalizálni, hiszen a támadó gépek számának növelésével növekszik annak az esélye, hogy a támadás előkészítése vagy végrehajtása során kiléte kiderül. A minimalizálás mellett viszont olyan mennyiségű forgalmat kell generálnia, amely alkalmas a célszámítógép túlterhelésére. Ennek megfelelően a támadó által használt munkaállomások rendszerint nagyobb forgalmat generálnak, mint a legitim



2. ábra. Vírusvédelmi rendszer DOS védekezés prototípusa

munkaállomások.

A támadó forgalom kitiltása

A felismert támadóktól a leveleket (megfelelő időn át) nem fogadjuk el. Amennyiben ily módon véletlenül legitim felhasználókat is kitiltottunk, úgy ezek a felhasználók az SMTP protokoll hibatűrése folytán később még megpróbálhatják leveleik elküldését. A rendszer ezért robosztus: A levelek még akkor sem vesznek el, ha téves pozitív választ adna védelmi rendszerünk.

A védekezés sikerének ellenőrzése

A védekezés sikerességének ellenőrzése természetesen a forgalom vizsgálatán alapul: Amennyiben a forgalom megfelelő mértékben csökken egy elfogadható szintre, úgy a védekezést sikeresnek tekinthetjük. Amennyiben a védekezés nem sikeres, úgy a B. C. illetve D. pontok újbóli alkalmazása válhat szükségessé.

Prototípus

A DoS védelmi rendszerre prototípust készítettünk el, mely a 2. ábrán látható. A mintaimplementáció több részből áll: A Bernstein-féle UCSPI-TCP csomag átírt RBLSMTPD komponense fogadja a levelezést, és adja tovább az EXIM felé a beérkezett kapcsolatokat. Az Exim-re épülő antivirus struktúra képezi a védett rendszert. Ez egy

amavisd-new vírusszűrő modult használ (MTA-Scanner middleware), amely ClamAV illetve egy másik kereskedelmi vírusirtó segítségével védi a levelezést.
A forgalmi analízis a átírt TCP Wrapper (RBLSMTPD, itt aDoSSMTPd) segítségével zajlik. A rendszer másik komponense az általunk aDoSd-nek hívott statisztikai adatgyűjtő mag. Az TCP Wrapper (ADoSSMTPd) egy Unix domain socket segítségével kérést intéz a statisztikai maghoz, hogy az adott IP szám küldhet-e levelet. Erre a statisztikai mag a szűréseknek megfelelően visszajelez, illetve frissíti belső statisztikai komponenseit. (Tárolja a kérést).
A statisztikai mag rendszeresen, jelenleg 2 másodpercenként összegzi statisztikai eredményeit és elvégzi a kívánt vizsgálatokat a fentebb ismertetett algoritmusok szerint.

A statisztikai magot a könnyebb bővíthetőség és átláthatóság érdekében PERL-ben írtuk meg. A statisztikai mag természetesen naplózást is végez, illetve egy külön kis programocska segítségével adatok kérdezhetőek le belső állapotváltozóinak jelenlegi értékeiről.

Működőképesség

A jelenlegi prototípust egyelőre teszt üzemben vizsgáltuk meg. Hamar kiderült az, hogy a levelezési forgalom egyes specialitásai az [1] publikációban ismertetett algoritmusok megváltoztatását igénylik. A levelezés forgalma hajlamos burst-ök kialakulására, amelyek az ablakméretek jó kalibrálását igénylik, illetve a kis forgalmú szakaszokban szükséges az algoritmus olyan korlátozása, hogy bizonyos minimális forgalom alatt ne tekintsen támadásnak egy hirtelen forgalmi ugrást (éjjeli üzem).

Vírusok

A prototípus véleményünk szerint nemcsak a DoS támadók, de a vírusok ellen is hatékony lehet. Amennyiben egy munkaállomás megfertőződik, és elkezdi terjeszteni saját magát, úgy a forgalmi ugrás alapján a DoS védelmi rutinok ezt támadásnak ítélhetik, és az illető állomást kitilthatják. A kitiltásról a rendszergazda értesítést kaphat, és felderíthető, hogy mi volt a tiltás valódi oka, felfedezve a vírust. A rendszer érdekessége, hogy mivel a forgalom analízisére épül, így a még ismeretlen vírusok is felfedezhetőek, illetve a detektált támadások összefoglalhatóak egy nagyobb, disztributív rendszerbe is, amely alkalmas lehet a vírusjárványok korai detekciójára és a hatékonyabb ellenintézkedések elvégzésére.

Természetesen elképzelhető olyan eset is, amikor nem támadó, és nem is vírus okoz vélt támadást, hanem egy vagy több belső vagy külső felhasználó körlevele indítja be a támadást érzékelő algoritmust.
A rendszer ez ellen úgy védhető, hogy adott állomások ún. „white list” módszerrel a statisztikai magból kikerülhetnek, ezeknek joguk van bármilyen mennyiségű levél küldésére. Másrészt gyakran előfordul, hogy a túlterhelést hasonló módon belső felhasználók legitim levelei okozzák. Ilyen esetben a rendszer a felhasználót egy időre ki

tudja tiltani, aminek eredményeképpen a felhasználó figyelmeztethető. Hasonlóképpen a tiltás lejártával a felhasználó számítógépe a körlevelet el tudja küldeni azokhoz a címzettekhez, akikhez az előző futás alkalmával nem sikerült, így a levelek nem vesznek el, viszont megkíméltük szerverünket egy esetleges túlterheltségtől.

Összefoglalás

A fentiekben bevezetést kívántunk nyújtani a vírusvédelem legnagyobb problémáira, amelyeken csak a rendszerszemléletű, összehangolt védekezés segít. A védekezési módszerek rövid felsorolása mellett be kívántuk mutatni néhány olyan projektünket, amelyek célja a fenti problémák megoldása, illetve a megoldás támogatása.
Fontos felismerni és elismerni, hogy egy-egy megoldás nem fogja megoldani az internetes problémák egyikét sem (vírusok, DoS támadások, spam, stb.), de a megoldások megfelelő kombinálása, széleskörű és koordinált alkalmazása segíthet a problémák kezelésében.

Hivatkozások

[1] B. Bencsáth, I. Vajda, Protection Against DDoS Attacks Based On Traffic Level Measurements, 2004 International Symposium on Collaborative Technologies and Systems, 2004, edited by Waleed W. Smari, William McQuay, pp. 22-28., The Society for Modeling and Simulation International, San Diego, CA, USA, January, Simulation series vol 36. no. 1., ISBN 1-56555-272-5

[2] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. In Advances in Cryptology -- Crypto '92: 12th Annual International Cryptology Conference, Proceedings, Lecture Notes in Computer Science volume 740, pages 139-147, Santa Barbara, California, August 1992. Springer.

[3] B. Bencsáth, L. Buttyán, I. Vajda, A game based analysis of the client puzzle approach to defend against DoS attacks, Proceedings of SoftCOM 2003 11. International conference on software, telecommunications and computer networks, 2003, pp. 763-767,

[4] Ioannidis, J. and S. M. Bellovin. "Implementing Pushback: Router-based Defense Against DDoS Attacks." In Proceedings of Network and Distributed System Security Symposium, Reston, VA, USA, Feb. 2002, The Internet Society.

[5] B. Bencsáth, I. Vajda, Trap E-mail Address for Combatting E-mail Viruses, Proceedings of SoftCOM 2004, FESB Split, 2004.