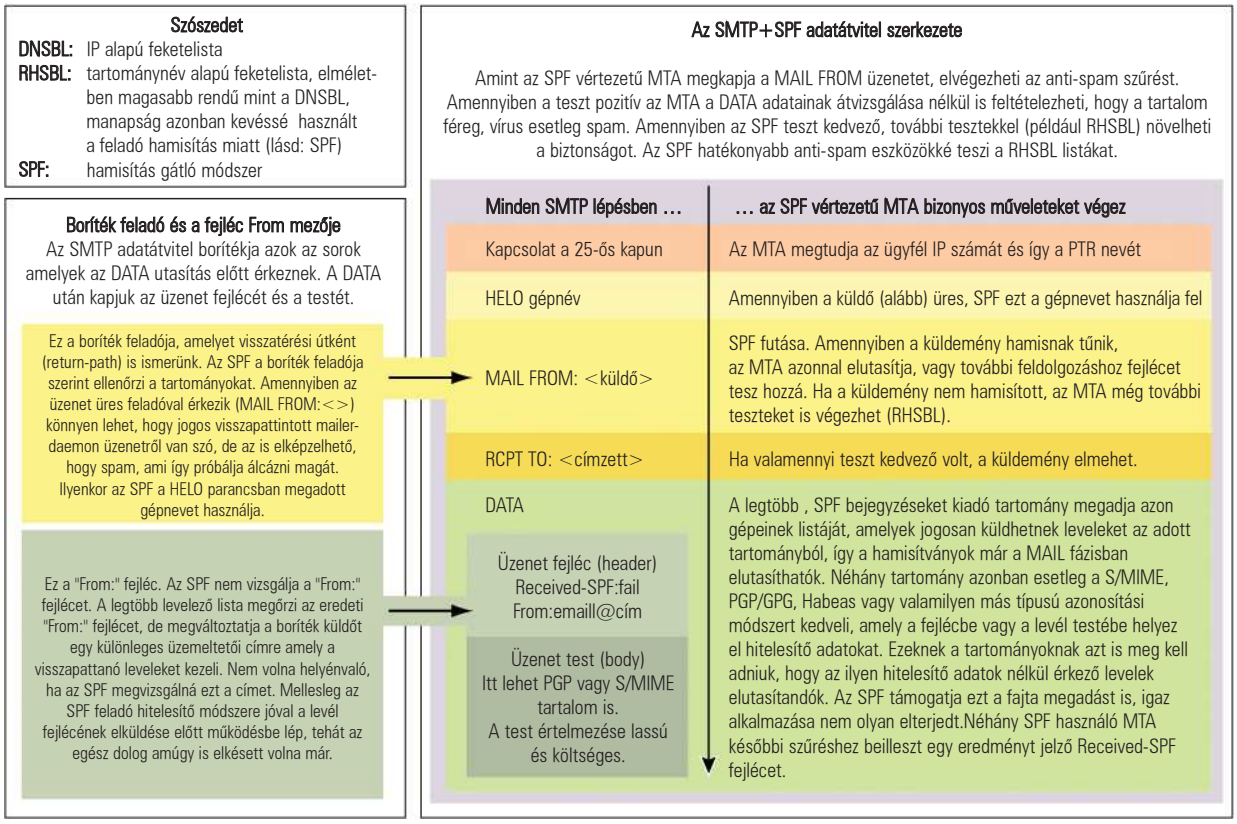
SPF bemutató

A szemétlevelek (spam) által okozott problémák kezelésében nagy segítséget nyújthat, ha időben felfedezzük a hamisításokat. Őrizzük meg e-mail címünk jó hírét egy egyszerű DNS technika segítségével.

Az SPF (Sender Policy Framework) egy új és egyre népszerűbb hamisítás-ellenes szabvány, melynek célja, hogy a különféle férgek, vírusok és szemétlevelek ne tudjanak tetszőleges e-mail címet írni az SMTP levélboríték „küldő” mezőjébe. Két fő részből áll: a tartománygazdáknak a DNS-ükön elérhetővé kell tenniük az SPF bejegyzéseket, az e-mail gazdáknak pedig SPF kézelérésre képes MTA-t kell alkalmazniuk, amelyek felhasználják ezeket az adatokat. Az SPF bejegyzések azt a gépet azonosítják ahonnan a tartomány kimenő levelei érkeznek. Bármilyen más helyről érkező levél hamisítottnak számít. E kétrészes cikk első részében az SPF alapjaival és kompromisszumaival ismerkedhetünk meg, valamint megtudhatjuk, hogy a DNS gazdáknak miképpen kell beállítaniuk az SPF bejegyzéseket. A második cikk inkább az e-mail rendszergazdák számára készül, és azt mutatja be, hogyan kapcsolhatják be az MTA SPF védelmet. A cikk 2004 január elején született, ennek megfelelően az Internet akkori állapotát tükrözi.

Férgek, Vírusok, Joe-Job módszerek és boríték feladó hamisítás

Ma saját magamtól kaptam spamet. Én alapítottam a ➲ http:\\www.pobox.com-ot, és értek az e-levelekhez. Gyorsan rá is csaptam a H billentyűre, hogy lássam a fejlécet és megvizsgáljam a Received sorokat. Ahogy gyanítottam: mint az általam kapott legtöbb spam, ez is egy szélessávú hozzáféréssel rendelkező gépről jött. Valószínűleg egy javítatlan Windows 2000-et futtató, játékra és mp3 hallgatásra használt öreg PIII-ról lehet szó, mely koszos alsóneműk halma alatt csendesen zümmög valakinek az ágya mellett. De az is lehet, hogy egy Idaho-i krumplifarmon zörög, vagy esetleg a Central Park-ra van szép kilátása. Akárhogy is, valószínűleg megfertőzte a spammelőkkel együttműködő Sobig vírus valamelyik variánsa. A gép jogos tulajdonosának fogalma sincs róla, hogy gépét megfertőzték, nem tudja, hogy gépe óránként jó néhány ezer levelet és vírust küldözget szerte azóta a rég elfelejtett nap óta, amikor az a különös csatolmány nem akar megnyílni, hiába böködte.
A spam üzenetek elrejtik valódi származási helyüket. A spammelők megrontott gépeket használnak az üzenetek szétküldésére. Hamisítják a levélfejléceket. Átírják a Received fejléceket, hogy becsapjanak. Hibás Tárgy-at fabrikálnak, hogy átejtsék a statisztikai szűrőket és meghamisítják a `>From` sorokat, eljátszva, hogy leveleiket a PayPal vagy az eBay küldte.
A spammelők gyakran a visszatérési utat is meghamisítják. Amikor a levél kézbesíthetetlen, visszapattan az eredeti feladóhoz, akinek a címe a visszatérési útban található. Itt nem a levélfejléc From: címéről van szó, hanem az SMTP boríték visszatérési címéről, az RFC2821 MAIL FROM mezőről. A spammelő program gyakran használ régi címeket, esetleg egyszerűen csak megpróbál kitalálni néhány gyakran használt nevet, vagy szótártámadást indít. Az eredmény rengeteg hibás és visszapattanó levél.
A spammerek nem szeretnék ezeket megkapni. Sokkal jobban tetszik nekik, ha valaki más kapja meg őket. Ezért véletlenszerűen kiválasztanak egy címet, vagy egyszerűen a címzettet írják ide. Ez az oka, hogy úgy nézett ki, mintha magamtól kaptam volna spamet. Néha valamelyik gyűlölt ellenségük címét írják be, készakarva behamisítják a címét így aztán elárasztják majd a visszapattanó levelek ezrei.
1997-ben valaki a levelek visszatérési címébe a ➲ http:\\www.joes.com címét hamisította, amit aztán annyi levél árasztott el, hogy tíz napra leállt – innen a művelet neve: joe-job. A Hotmail és az AOL minden nap küzd ezzel a problémával: rengeteg spammer hamisít a levélbe AOL címet, de valójában persze nem az ő kiszolgálóikat használja. Hagyományos SMTP eszközök segítségével az AOL semmit sem tehet ez ellen. Ha egy pólóra nyomnánk az AOL logót és megpróbálnánk eladni azt, egy szemvillanás alatt a nyakunkon volna az AOL összes ügyvédje. A spammelők ugyanakkor naponta hamisítják a @aol.com címet. És ezzel nekik együtt kell élniük, mert SMTP-t használnak. Az Simple Mail Transfer Protocol (SMTP) több mint húsz éve született – egy barátságosabb, kedvesebb világban. Az egész Internet Maroknyi kutatási intézményből állt. Az SMTP azóta is jól szolgál minket, de már mutatkoznak rajta az öregség jelei. Az SMTP nyílt és hiszékeny. Szabályai viszonylag kötetlenek. Bármilyen levélküldőt beilleszthetünk, és tetszőleges fejlécet komponálhatunk. Felmerül a kérdés, hogy manapság egy olyan protokoll, ami lehetővé teszi a joe-job féle cselekedeteket, vajon nem túl nyitott és hiszékeny-e. Ezért kellett kitalálni a feladó-azonosítást: Az SPF kicsit komolyabb szabályokat vezet be.



1. ábra Az SPF segítségével a levelező kiszolgáló ellenőrizni tudja, hogy a másik kiszolgáló ténylegesen azt a címet használja, amelyet a levélben állít

SPF alapú feladó azonosítás

Amikor levelünket elküldjük valamelyik tartománynak, MTA programunk egy DNS keresés (MX lekérdezés) segítségével találja meg, hogy melyik kiszolgálóra kell továbbítani a levelet. Az ilyen kiszolgálót levélcserélőnek hívjuk (mail exchanger, röviden MX). Az apró tartományoknak többnyire csak egy MX kiszolgálójuk van, a nagy tartományok általában többet tartanak fenn. A tartományra érkező levelek annak MX kiszolgálójára érkeznek be.

Lássuk akkor a nagy ötletet. Az esetek 99%-ában, amikor a tartomány elküldi a levelet, a levél a tartomány által irányított viszonylag kis számú kiszolgálóról származik. Tekintve, hogy a tartomány ezeknek a kiszolgálóknak nyújt DNS szolgáltatást, bármely, más helyről érkező levelet valószínűleg hamisnak tekinthetünk. Ezt a módszert célzott feladó-sémának nevezzük (designated sender scheme, *1. ábra*).

A célzott feladó séma fő előnye, hogy segít elhárítani a hamisítókat, ráadásul nagyon egyszerű megvalósítani. Végtére is a tartománygazdák már eleve tudják, milyen kiszolgálók küldenek leveleket az adott tartományból. Amikor azt mondom „levelet küld a tartományból" , az SMTP küldemény forrását értem alatta, azaz a boríték MAIL-FROM feladó mezőjében található kiszolgálót. Nem a From: fejlécről van itt szó. Ez nagyon fontos különbség.

A tartományból érkező levelek általában kis számú kiszolgálóról érkeznek. Ez a kis és nagy tartományokra egyaránt igaz. Az aol.com levelei az AOL kiszolgálóiról jönnek. A saját tartományom levelei természetesen a saját tartományom kiszolgálóiról. Mindenesetre biztosan nem jönnek valami koszos alsóneműkkel fedett gépről.

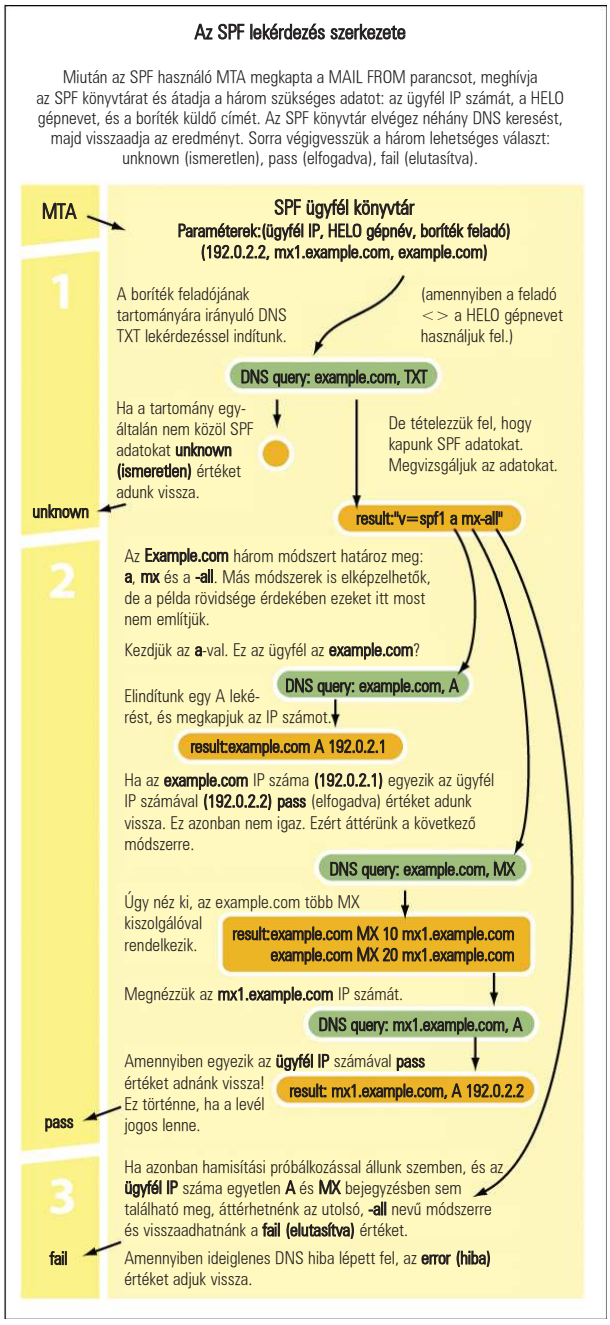
Sok ISP már ma is alkalmaz hasonló szabályokat, bár eléggé esetlegesen és gyakran kicsit hibásan. Az a gond ugyanis, hogy az egyik ISP nem igen ismeri a másik ISP belső világát, így gyakran hoz rossz döntést. Például az aol.com levelező-kiszolgálói elképzelhető, hogy az aol.net tartományba is tartozhatnak, vagy fordítva. Nem lenne sokkal egyszerűbb, ha az AOL saját maga adná meg a kiszolgálói nevét valamilyen egyszerű, rugalmas, bővíthető nyílt formátumban, amit bárki felhasználhat?

Nos, pontosan ezt teszik. Az SPF szabványos, rugalmas, bővíthető és nyílt formátum, amit bárki használhat. Az AOL pedig épp mostanában kezdte el közzétenni saját SPF bejegyzéseit. Az MTA-k értelmezhetik ezt a bejegyzést, melynek segítségével már el tudják dönteni, hogy a levél valóban a @aol.com tartományból érkezik, avagy hamisítvány. Ez az egész szigorítás teljesen önkéntes: azok a tartományok, melyek nem tesznek elérhetővé SPF bejegyzéseket, továbbra is ugyanúgy elküldhetik a leveleiket. Néhány szokatlan tartomány esetleg jobban működik, ha nem ad ki ilyen bejegyzéseket; rajtuk áll mit szeretnének. A legtöbb tartomány valószínűleg szívesen használná az SPF előnyeit.

A SPF bejegyzések felajánlásához a tartománynak mindössze egyetlen bejegyzést kell a zóna állományhoz adnia. A bejegyzés szöveges sor, akár ma is összerakhatjuk. Nézzük meg, hogyan is néz ki ez a bejegyzés.

SPF példa

Tegyük fel, hogy a ➲ http:\\www.example.com SPF bejegyzéseket akar felajánlani. Szeretné, ha a világ MTA-i elolvasnák az SPF bejegyzéseit és ennek alapján elutasítanák a ne-



2. ábra Az SPF minden bejövő levélre egyszerű DNS-alapú keresést alkalmaz

vében hamisított leveleket. Reméli, hogy az SPF segítségével csökkentheti a viaszpattanó joe-job levelek és hibás figyelmeztetések számát. Ezért zóna állományához a következő sort adja hozzá:

```
example.com.  IN TXT  "v=spf1 a mx ptr -all"
```

A `v=spf1` verzió azonosító mutatja, hogy SPF bejegyzésről van szó. A `-all` jelentése: alapértelmezés szerint minden levelet utasítsunk el. Azok a tartományok, amelyek egyáltalán nem küldenek levelet, az egyszerű `v=spf1 -all` alaknál meg is állhatnak. Ha azonban a tartomány szeretne leveleket is küldeni, meg kell adnia a módszert, amellyel eldönthető hogyan kell kinéznie egy hiteles levélnek. A módszer középre kerül, az `-all` kapcsoló elé. Az SPF lekérdezés eredménye az első egyezést mutató módszer lesz, mivel a `-all` mindennel megegyezik, a végére kell helyeznünk.

A módszereket balról jobbra értelmezzük. A `v=spf1` a `mx ptr -all` sorozat alkalmazásakor először megvizsgáljuk, hogy a kapcsolódó ügyfél megtalálható-e a tartomány A bejegyzései közt, avagy ha itt nem találjuk meg, az MX kiszolgálók listájában. Ezek után az MTA leellenőrizheti, hogy az ügyfél gépneve egyezik-e a tartománnyal. Ha egyik módszer sem ad eredményt, a `-all` értékelődik ki, és az MTA jogosan elutasíthatja a levelet.

Az A, MX, PTR és IP4 kulcsszavak a tartományok nagy többségének bőségesen elegendőek. A `spf.pobox.com/wizard.html` beállítás-varázslója segít nekünk megalkotni a saját tartományunkhoz tartozó SPF bejegyzést. Amennyiben a mi problémánk összetettebb, kipróbálhatjuk a „Advanced SPF” széljegyzet alatt leírtakat.

Egyszerű SPF

A: Az A módszer lényege, hogy az example.com IP címéről szabad az example.com-ról érkező leveleket küldeni. Ha azt akarjuk megadni, hogy a valami-más.com IP címét is engedélyezzük, a következőket írjuk: `a:valami-más.com`. Annyi A bejegyzést alkalmazhatunk amennyit csak akarunk.

MX: Az MX módszer jelentése, az example.com minden MX kiszolgálója jogosan küldhet levelet az example.com tartományból. Amennyiben a valami-más.com MX kiszolgálóit is engedélyezni szeretnénk, adjuk ki a `mx:valami-más.com` utasítást. Annyi MX bejegyzést használhatunk, amennyit csak szeretnénk.

PTR: a PTR módszer lényege, hogy amelyik a gép example.com-ra végződő PTR bejegyzéssel rendelkezik, jogosan küldhet levelet az example.com tartományból. Jó választás lenne ez például a Yahoo-nak, melynek minden kiszolgálója yahoo.com-ra végződik. Ugyanakkor nem túl jó választás a Comcast Borland szolgáltatónak. Amennyiben azt szeretnénk, hogy a valami-más.com végződésű kiszolgálók is küldhessenek leveleket az example.com tartományból, adjuk meg a `ptr:valami-más.com` kifejezést. Tetszőleges számú PTR mechanizmust használhatunk.

IP4: Tegyük fel, hogy a `192.0.2.0` számú C osztályú hálózat jogosult küldeni levelet az example.com tartományból, ilyenkor az `ip4:192.0.2.0/24` kifejezést kell bevinnünk.

Bővíthetőség

Az SPF számos beépített lehetőséggel rendelkezik. A legalapvetőbbek segítségével megadhatjuk a tartományunkból levelet küldő gépek címeit. Ez a funkció szinte minden tartomány számára elegendő, hiszen minden tartomány levelei gépek viszonylag kis csoportjától érkeznek. De ha a tartományunkról érkező leveleket valamilyen más módon külön-

Továbbfejlesztett SPF

Exists: az Exists módszer tartománynevekre ráhúzható kifejezéseket használ, ahol makrókat is használhatunk. Például, az `exists:%{ir}.%{l}._spf.example.com` ráhúzható a `2.2.0.192.ceo._spf.example.com` névre. Az SPF ügyfél A lekérdezést fog végrehajtani a ráhúzott tartománynévre, és ha visszakap valamilyen A bejegyzést (például 127.0.0.2) az Exists megadja az engedélyt. Ezt a technikát alkalmazhatjuk például, amikor szeretnénk, hogy a ceo@example.com különleges felhasználó egy adott gépről, mondjuk a 192.0.2.2-es címről leveleket tudjon küldeni, miután létrehoztuk a fenti tartománynévnek megfelelő A bejegyzést. Vannak, akik saját DNS kiszolgálót készítenek az összetett Exists lekérdezések kezelésére. Az Exists felhasználásával a határ a csillagos ég.
Include: ha leveleinket egy másik szervezet kiszolgálóin keresztül küldjük, az Include segítségével adhatjuk meg a tartományt, így a megfelelő SPF bejegyzés hívódik és helyettesítődik be. Például, ha a vanity tartomány az ISP.com levelező kiszolgálóin keresztül küldi a leveleit, használhatja az include:isp.com bejegyzést. Bármely kiszolgáló, amely leveleket küldhet az ISP.com tartomány nevében, ezt követően jogosult lesz a vanity tartományt is használni. Az include-dal több tartományt is megadhatunk.
A Redirect és az Exp: módosítók az eddig látott egyéb megoldásoktól némiképp eltérőek; kettőspont helyett egyenlőség jelet használnak. Bár a módszerek megismételhetők, egy SPF bejegyzésben csak egy módszerünk lehet. A `Redirect` módosító hasonlóképpen működik, mint az `Include`, azzal a különbséggel, hogy az eredeti kérelmet teljes egészében helyettesíti az új bejegyzés. Az `Exp` megadásával leíró szöveget adhatunk meg. Ha az MTA elutasítja a hamisítási kísérletet, az itt megadott leíró szöveg jelenik meg az eredeti feladónak visszaküldött SMTP hibaüzenetben. Lehetnek jogos felhasználóink, akik nem az általunk megadott SMTP kiszolgálókat használják, az SPF hamar kideríti kik is ők. A leíró szöveget egy URL-re is állíthatjuk, ahol a levelező ügyfél helyes beállításaival kapcsolatos további információkat helyezünk el. Az itt bemutatott módszerek részletes leírását az ➲ http:\\www.spf.pobox.com/mechanisms.html címen találjuk.

SPF és hagyományos Antispam módszerek

A DNS feketelisták vagy gátlólisták (blocklist, DNSBL): Az IPv4 tér 32 bit széles; 2^{32} körülbelül 4.2 milliárd – 4.2 milliárd homokszem megtöltene egy dömpert. Képzeljük el, hogy valamennyi homokszemet feketére vagy fehérre festjük. Az IP-alapú feketelista derék próbálkozás, de túlságosan alacsony szinten próbálja kezelni a problémát. A jó DNSBL rendszernek el kell döntenie, hogy az adott IP cím spammelő vagy sem, csakhogy helyesen kell döntenie mind a 4.2 milliárd IP cím esetében. Ne csodálkozzunk rajta, hogy a DNSBL listák jönnek-mennek. A fenntartóik idővel belefáradnak és feladják.
Jobboldali feketelisták: az RHSBL tartománynéveket használ, a DNSBL IP címeket. A tartománynevek sokkal alkalmasabbak az internetes objektumok azonosítására, azonban a RHSBL listák még nem olyan népszerűek, mint a DNSBL táblák. Vajon miért? A spam soha nem jön a spammer.net-ről. Sokkal valószínűbb, hogy a yahoo.com címet hamisítják. Ez az ahol az SPF segíthet: ha a spammelők valódi nevükről küldik a leveleket, feltartóztatásuk is egyértelművé válik.
Címellenőrzés: a MAIL fázisban leellenőrizhetjük a boríték feladóját, ha megpróbálunk levelet küldeni neki. Ha a próbaüzenet címzett ismeretlen üzenettel tér vissza, nem fogadjuk el az üzenetet. Ez azért hasznos, mert a spammelők gyakran választanak véletlenszerű címeket. Azonban ahogy a címellenőrzés egyre általánosabbá válik, a spammelők is várhatóan létező címeket fognak hamisítani-még egy érv az SPF mellett.
Aláírás alapú megoldások: a PGP/GPG és S/MIME felhasználók aláírják üzeneteiket. A fogadó a kulcs kiszolgálóról letöltött kulcsokkal ellenőrizheti az üzenet hitelességét. Olyan szerekezeteket is javasoltak, ahol maga a DNS működne a nyilvános kulcsok tárházaként. Ezek a megoldások azért hasznosak, mert a .forward állományok módosítás nélkül működhetnek tovább. Ugyanakkor hátrányuk, hogy a hitelesség ellenőrzéséhez a levélnek keresztül kell haladnia a csővezetéken, így sávszélességet és CPU időt használ el. Mindenesetre a fenti módszerek bármelyikét alkalmazó tartomány használhatja az SPF módszert annak megadására, hogy minden aláírás nélküli üzenetet el kell utasítani.
Válasz: Nyilván nem szeretnénk válaszolni egy spamre, különösen nem egy hamisított spamre. Ha az SPF megmutatja nekünk, hogy a küldő címe egyértelműen hamis volt, nyugodtan törölhetjük a levelet anélkül, hogy válaszolnánk rá.

böztetjük meg, mondjuk mindig S/MIME jellel látjuk el őket, a megszokott `a` vagy `mx` helyére az `smime` kódot kell írnunk. A küldő azonosítás egyik megközelítési módja a dedikált feladó mechanizmus (designated sender mechanisms) kialakítása (A, MX, PTR és IP4). Újfajta küldő-azonosítási módszerek is kialakulóban vannak. Az SPF bővíthető, így majd ezekkel is együtt tud működni. A jövendőbeli mechanizmusokat értelmező SPF bővítmények már helyesen fogják tudni értelmezni őket. Azok az SPF bővítmények amelyek nem értették meg az új mechanizmust, ismeretlennek fogják tekinteni, és úgy veszik, mintha a tartományunknak egyáltalán nem lenne SPF bejegyzése.

Az Altartományok és az MX kiszolgálók védelme

Manapság a spammelők tartományneveket hamisítanak. Lehet, hogy hamarosan gépneveket hamisítanak. Lehet hogy megpróbálják joe-job módszerrel célba venni a laptopunkat, kipróbálva az username@ibook.example.com címet. Ezért nem árt ha az altartományunkat is megvédjük. Kezdjük az MX kiszolgálókkal, majd térjünk át az összes A bejegyzéssel rendelkező gépre. Lássuk miért.

A visszapattanó levelek küldő mezőjében a `MAIL FROM: <>` üzenetet találjuk. A nullfeladó-cím biztosítja, hogy visszapattanó levelek ne pattanjanak vissza újra, és ne hozzanak létre ciklust. Amikor az SPF üres feladó címet lát, visszatér a `HELO` parancsban megadott címhez. Amikor a saját MTA-nk küld visszapattanó levelet, a gépnevet megadja az elküldött `HELO` parancsban. Ha ez a gépnév megtalálható az SPF rendszer listájában, az üzenet átmehet. Az SPF tehát egyúttal a `HELO` hamisítást is meggátolja.

Utazó Postás (Mailman) és továbbítási problémák

Az SPF célja: legtöbb hasznot hozni a lehető legolcsóbban. Megszigorítja a szabályokat, így a huligánok nehezebben tudnak rossz dolgokat művelni, mindeközben nem zavarja a jó embereket, akik jó dolgokat tesznek. Néhány komolyabb felhasználó, aki ki szeretné használni a SMTP laza szabályait, elképzelhető, hogy kényelmetlennek találja az SPF rendszerét. Ebben a szakaszban bemutatjuk, milyen problémákat okozhat az SPF a komoly felhasználóknak, valamint megnézzük hogyan kerülhetjük ki őket.

A legtöbb felhasználó a leveleit az ISP SMTP kiszolgálóin keresztül küldi ki. A legtöbb modern ügyfél támogatja a SASL azonosítási módszert vagy, ahol a felhasználóknak kívülről kell betárcsázniuk az ISP hálózatára, a POP-before-SMTP eljárást. Azok a felhasználók akik miden levelüket az ISP SMTP kiszolgálóin keresztül küldik, automatikusan SPF-kompatibilisek, azaz semmit sem kell tenniük.

Csakhogy néhány komoly felhasználó, aki a laptopján saját MTA-t futtat véletlenszerű IP címekről is küldhetik a leveleket, és így teljes mértékben kikerülik az ISP kiszolgálóit.

Az SPF ezen felhasználók igényeihez is alkalmazkodik: a továbbfejlesztett mechanizmus (lásd a „Továbbfejlesztett SPF” széljegyzetet) lehetőséget ad bizonyos felhasználóknak, hogy ne kelljen az ISP SMTP kiszolgálóit használniuk. Továbbra is azt tehetnek, amit akarnak.

Vannak komoly felhasználók, akik tucatnyi vagy még több címet használnak, amelyeket aztán `/etc/aliases` bejegyzésekkel vagy *.forward* állományokkal irányítanak egy helyre. A klasszikus átirányítás elvei szerint a boríték küldője változatlan marad és csak a címzett címe íródik át. Ez azonban problémát jelenthet, amikor az üzenet megérkezik a rendeltetési helyére – ugyanis továbbra is az eredeti feladó címet tartalmazza, így az SPF teszt hamisnak minősíti.

A megoldás szerencsére nem nehéz, egyszerűen csak át kell váltanunk újrapostázásra, ahol a küldő címe is átíródik. Ezt rengeteg módon megtehetjük. A nekünk legmegfelelőbb megoldást az SPF FAQ (spf.pobox.com/faq.html#forwarding) leírásából választhatjuk ki. A legtöbb végfelhasználónak nem sokszor akad dolga a továbbítással, inkább csak a komolyabb felhasználóknak van szükségük ilyen megoldásokra. Amennyiben harmadik fél által nyújtott szolgáltatást használunk az alumni, vanity tartományon vagy egyéb üzleti továbbító szolgáltató (pobox.com) gépén keresztül, elvárhatjuk, hogy meg tudják oldani nekünk az újrapostázást.

Spam feltartóztatása: Ez is a megoldás része

Az SPF elsődleges célja a hamisítás megakadályozásának további előnyei is vannak. Nem szeretnék több spamet kapni saját magamtól, és nyilvánvalóan nem szeretném, ha te kapnál olyan spamet, ami azt állítja, hogy én küldtem. A férgek és vírusok általában szintén hamisítják a küldő címét, így ezeket is megállíthatjuk az SPF segítségével. A hamisítás megakadályozása egy további előnnyel is bír. Ha a spammelők kénytelenek a saját nevüket használni, meg tudjuk állapítani mely tartományok jogosultak és melyek spammelők. Vannak, akik már most is ezt teszik: A jobboldali blokkolási listák (RHSBL) a DNS blokkolási listák (DNSBL) névkiszolgáló alapú változatai. Azok a spammelők, akik nem félnek saját tartományukat használni hamar az RHSBL listákon találják magukat, így könnyedén megállíthatjuk őket. Az SPF alapú világban az RHSBL sokkal fontosabbá és hatékonyabbá válna.

Miért használjuk az SPF-et?

A nagy tartományok, például az ISP-k, bankok, jól ismert cégek szeretik saját maguk irányítani a cégjelüket. Szinte kötelességük megvédeniük a nevüket. Az ➲ http:\\www.altavista.com éppúgy terjeszt SPF bejegyzéseket, mint az AOL és az Oxford. Minden nap új és új tartományok lépnek be az egyre bővülő körbe. A kisebb tartományok egyszerűen azért használnak SPF rendszert, mert nem szeretnének joe-job áldozatokká válni.

A fogadói oldalon az ISP-k MTA fejlesztésekbe kezdenek, és persze szívesen használják az SPF-et hiszen így kevesebb a hamisítás, ezzel együtt kevesebb spam, vírus és féreg. A sávszélesség költségük is lecsökken, hiszen az SPF segítségével még az adat elküldése előtt lecsaphatnak a spammelőre. Nincs szükség semmilyen titkosításra, ellenőrzésre vagy aláírásokra. Az SPF pénzt takarít meg.

Adaptálás

Mire ez a cikk megjelenik, az SPF támogatás már valószínűleg beépített része, vagy letölthető modulként elérhető lesz a legfrissebb SpamAssassin, Postfix, Sendmail, Exim és qmail terjesztésekben. Az üzleti antispam-terjesztők az SPF támogatása mellett döntöttek; egyikük, a Declude JunkMail, jelentette, hogy az SPF éles környezetben is sikeresen megállítja a kéretlen leveleket.

Ha minden jól megy, az SPF szabvány a közeljövőben RFC szabvánnyá válik. Több ezer tartomány, köztük néhány igazán nagy, azonban már most is terjeszti az SPF listákat. Nincs okunk várni; már ma érdemes kiadni saját SPF bejegyzéseinket.

Linux Journal 2004. április, 120. szám

Meng Weng Wong a pobox.com e-mail továbbító cég alapítója és CTO-ja, amely tizedik évfordulóját ünnepli ez évben. Jelenleg science-fiction novellasorozatán dolgozik, amely olyan bolygón játszódik, ahol Clarke híres elképzelése nyomán, nanotechnológiával valósították meg a fantasy mágiát.