A Magyarországon alkalmazott spamszűrési módszerek és a Sender ID

Szabó Gábor
Szabó Géza
2005. január 30.

Kivonat:
Az alábbi cikkben röviden áttekintjük az újradolgozott Sender ID Framework működését, kombinálhatóságát a Yahoo's DomainKeys módszerével. A felmerülő kérdések elemzése után megindokoljuk mekkora lehetőség nyílhat az elterjedésükre elsősorban Magyarországot tekintve.

1. Bevezető:

Napjainkban az e-mail-forgalom növekedésével folyamatosan nő a hálózatot terhelő kéretlen reklámlevelek (spam) száma is. A probléma akkora méreteket öltött, hogy már nem csak vállalati, hanem kormányzati szinten is harcolnak ellenük.
Szinte naponta kerülnek a piacra olyan termékek, amelyek 100%-os hatékonyságot ígérnek a spamek kiszűrésében, azonban a várva várt átütő siker mindezidáig elmaradt, miközben a probléma csak fokozódik.
Az alábbiakban bemutatásra kerülő módszereket elsősorban a kéretlen reklámlevelekkel elkövetett támadások egy speciális fajtájának, a domain spoofing-nak, illetve az ezzel összefüggő phishing-nek a megszüntetésére hozták létre. Domain spoofing alatt azt értjük, amikor a támadó (spam-et küldő) megváltoztatja az e-mail From: mezőjét, ezáltal megpróbálja magát legitim küldőnek feltüntetni. A phishing ennél annyiban jelent többet, hogy az ilyen módon meghamisított elektronikus levélben megpróbálják rábírni a címzettet valamilyen személyes adatának (elsősorban bankszámla számának, PIN kódjának) kiadására.
Fontos tehát már most kiemelni, hogy az ismertetésre kerülő módszerek nem fogják megszüntetni a kéretlen reklámlevelek minden formáját.

1.1. Az alapprobléma:

Annak eldöntését, hogy egy e-mail egy adott domain-hez tartozó-e, vagy sem, megfogalmazhatjuk egy döntési problémaként:
Adva van egy e-mail és egy IP cím, ahonnan ezt a levelet továbbították (vagy továbbítani fogják). A kérdés az, hogy az adott IP címhez tartozó SMTP kliens jogosult-e elküldeni az üzenetet?
Ezt a kérdést kell megválaszolnia egy SMTP szervernek annak eldöntéséhez, mit kezdjen egy bejövő e-maillel (továbbítsa a címzettnek, vagy esetleg dobja el).

2. A Sender ID Framework

2.1 A Sender ID Framework működésének rövid áttekintése:

A SENDER ID FRAMEWORK [1] [2] egy ipari szabvány, melyet az e-mail domain spoofing visszaszorítására, illetve magasabb szintű biztonsági szolgáltatások nyújtására hoztak létre.
Az eljárás kombinálja a Microsoft Caller ID for E-mail módszerét, Meng Wong SPF eljárását illetve egy harmadik specifikációt, a Submitter Optimizationt.
Az 1.1-ben ismertetett döntési probléma megválaszolására, illetve a döntés megkönnyítésére dolgozták ki a SENDER ID FRAMEWORK-t. Vagyis ebből már látszik, hogy az alap cél a küldő azonosítása, valamint nyilvánvaló, hogy ez csak címhamisítások ellen fog védeni.
Az eredeti Sender ID Framework egyszerű háromlépcsős folyamat:

1. Az e-mail küldők nyilvánosságra hozzák a kimenő e-mail szerverük IP címét a DNS-ben a Sender ID specifikációban megadottak alapján.
2. Az e-maileket fogadó szerverek megvizsgálnak minden egyes üzenetet, hogy meghatározzák a purported responsible domain-t (~bizonyított felelős domain), vagyis azt az Internet domain-t, mely az e-

mail küldéséért ”felelős”.

3. Az e-maileket fogadó szerverek lekérik a purported responsible domain DNS-ét, ezzel megkapják az ahhoz tartozó olyan IP címeket, melyek jogosultak onnan üzenetet küldeni. Ezek után ellenőrzik, hogy az az IP cím, melyről az e-mail érkezett, rajta van-e a lekért listán. Ha nincsen egyezés, akkor az e-mail valószínűleg spam.

A kezdeti lelkesedést követően egyre többen fejezték ki aggályaikat a módszert illetően. Az ellenzők érvei a következők voltak (a teljesség igénye nélkül):

- Számos technikai kérdés nincsen megoldva (forward-olás, levelező listák, stb.).
- Nem kompatibilis az SPF-vel, ami már elterjedtebb módszer.
- A licenc miatt a nyílt forráskódú implementáció nem megoldható.

Végül 2004. októberében az IETF (Internet Engineering Task Force) elutasította a szabványosítási kérelmet.

Ezt követően a Microsoft Safety Technology & Strategy Group-ja átdolgozta és egy újabb javaslattal állt elő. Ebben elsődlegesen az SPF-vel való kompatibilitást oldották meg, másrészt rögzítették azt is, hogy az egyéb kifogásolt szolgáltatások (forwardolás, levelező listák) hogyan valósíthatóak meg.

2.2. Az átdolgozott Sender ID Framework rövid ismertetése

Az újabb változat már választási lehetőséget kínál a PRA, illetve Mail From alapján történő ellenőrzés között. A működési folyamata tehát így módosul:

1. Az e-mail küldők nyilvánosságra hozzák a kimenő e-mail szerverük IP címét a DNS-ben SPF rekordként.
2. A fogadók megállapítják, hogy melyik domaint kell ellenőrizniük:
   a. A Purported Responsible Domain-t („Bizonyítottan Felelős Domain”), ami a levél törzséből határozható meg (RFC 2822 header).
   b. Az „Envelope From” domain-t (RFC 2821 Mail From).
3. A fogadók lekérik a kimenő e-mail szerverek DNS-ét a kiválasztott domain alapján és elvégzik a domain spoofing tesztet.

Ryan Hamlin (general manager of Microsoft’s Safety Technology and Strategy Group) az átdolgozott módszerrel kapcsolatban a sajtónak tett nyilatkozatában [5] azonban már arra is rámutatott, hogy a Sender ID Framework csak egy kezdeti lépés a spoofing és phishing problémák megoldására. A továbbiakban ők is egyéb hitelesítési eljárásokat, a digitális aláíráson alapul megoldásokat kívánnak alkalmazni. Konkrétan a Yahoo’s DomainKeys módszert emelte ki.

3. Microsoft’s Sender ID Framework és Yahoo!’s DomainKeys

3.1. A Yahoo!’s DomainKeys rövid ismertetése:

A Yahoo’s DomainKeys [4] [6] módszer a nyilvános kulcsú kriptográfián alapul, ezáltal kriptográfiai védelmet biztosít a nem hitelesített e-mail-ek ellen. A működése két részre bontható: a levelek aláírására, illetve az aláírás ellenőrzésére.

Küldő szerverek feladata (a levelek hitelesítése aláírással):

1. A domain-tulajdonos generál egy privát / publikus kulcs párt, amit a kimenő levelek aláírására fog használni (lehetőség van természetesen több kulcs pár generálására is). A nyilvános kulcsot mindenki számára hozzáférhetővé teszi a DNS-ben, míg a privát kulcsot csak a kimenő leveleket kezelő szerver ismeri.
2. Amikor a domain-on belülről egy hitelesített végfelhasználó küld egy e-mailt, a kimenő leveleket kiszolgáló szerver a titkos kulccsal generál egy aláírást az e-mailre. Ezt az aláírást csatolja a levél header részéhez és így küldi el a levelet a címzetthez.

Fogadó szerverek feladata (a hitelesség ellenőrzése):

1. Első lépésben a szervernek meg kell állapítania, hogy a levél mely domain-ból érkezett és az adott domain-nak le kell kérnie a nyilvános kulcsát.
2. Ezt követően a megszerzett nyilvános kulccsal ellenőrzi az aláírás hitelességét a szerver. Ezzel azt biztosítja a módszer, hogy ellenőrizni lehet tényleg abból a domain-ból érkezett-e az e-mail, valamint nem történt-e valamilyen változtatás időközben a levélben (elsősorban a header-t értik ezalatt).

3. Végül a szerver a helyi biztonsági előírásoknak megfelelően dönt a levél további sorsáról. Ha sikeres volt az aláírás ellenőrzés, akkor átveszi a levelet továbbításra, ha nem akkor megjelölheti, karanténba teheti, vagy akár el is dobhatja.

A módszer előnyei között a következőket emelik ki:

- Ha kellően hosszú kulcsokat alkalmaznak, akkor az azok feltörésére szánt költség nagyobb, mint a támadó vélt haszna.
- Az alkalmazás megoldható úgy is, hogy nem alkalmaznak CA-kat (Certification Authority). Ugyanis a domain-ek a DNS-ben hozzák nyilvánosságra a nyilvános kulcsokat, amihez akárki nem férhet hozzá, vagyis feltételezhető, hogy csak a domain tulajdonosa képes a nyilvános kulcsok publikálására.
- Levelezőlistákkal kapcsolatban sem merül fel probléma. Ha nem változtatják az e-mailt, csak továbbküldik, akkor nincs szükség különösebb intézkedésre. Ellenkező esetben pedig ők is aláírják a módosított e-mailt.
- Csak DomainKeys-vel rendelkező spammer képes spamet küldeni, akkor viszont mivel az adott kulcs egyértelműen tartozik valamilyen domainhez, be lehet azonosítani az illetőt (vagyis nem éri meg a spammer-nek, hogy saját DomainKeys-t hozzon létre). Ezzel a kérdéssel a 4. fejezetben részletesen foglalkozunk.

3.2. A két módszer együttes müködése:

Érdemes most azt összefoglalni, miként tud egymással együttműködni a Sender ID és a DomainKeys:

- *Közvetlen levéltovábbítás (Direct Delivery)*

A fogadó szervernek ellenőriznie kell a küldő domain DNS-ét. Így juthat hozzá a domain PRA-jához és a küldő nyilvános kulcsához. Ezt követően egyszerűen csak elvégzi mind a Sender ID tesztet, mind az aláírás ellenőrzését és ezek alapján dönt a levél további sorsáról.

- *Sender Agent-en keresztül (List Server, Mobile Carrier, Guest E-mail Service)*

Itt is a domain ellenőrzésével kell kezdenie a szervernek. Egyrészt a levél alapján meg kell határozni a levelező listát kiszolgáló szerver domain-t, valamint az eredeti küldőt is. Ezt a következők alapján teheti meg:

…
MAIL FROM:<owner-list@myownlist.com>
SUBMITTER=owner-list1@myownlist.com
….
From: alice@somewhere.com
Sender: owner-list@myownlist.com
To: list@somewhere.com
…

Mindegyiknek le kell kérnie a DNS-ét, hogy hozzájusson az adott domain PRA-jához és nyilvános kulcsához. Ezt követően mindegyikre el kell végezni a szükséges vizsgálatokat.

- *Recipient Agent-en keresztül (Forwarder)*

Ebben az esetben is ellenőrizni kell mind a küldő, mind a forwardolást végző szervert. A domain-ek azonosításához szükséges adatok az e-mail alábbi részei alapján határozhatóak meg:

….
MAIL FROM:<alice@somwhere.com>
SUBMITTER=bob@abc.def.edu
….
Resent-From: bob@abc.def.edu
….

Ezt követően itt is külön-külön el kell végezni az ellenőrzéseket.

- *Sender Agent és Recipient Agent együttes alkalmazása esetén (List Server + Forwarder)*

Az előzőek alapján már látható hogyan határozhatóak meg a keresett domain-ek.

Az eddigiek alapján azt lehet megállapítani, hogy egyrészt a Sender ID Framework-ben sikerült megoldaniuk az eddigi hiányosságokat, másrészt pedig könnyedén együtt tud működni a két módszer (nincsen szükség változtatásra egyik specifikációban sem).

3.3 A gyakorlatban felmerülő kérdések:

Vizsgáljuk meg, hogy a gyakorlati megvalósítással kapcsolatban milyen kérdések merülhetnek fel.

- A javaslat készítői előnyként emelték ki, hogy a Yahoo! DomainKeys módszer esetében nincsen szükség CA-k alkalmazására. Meg kell azonban jegyezni, hogy így szükség lenne DNSSEC alkalmazására, különben gondot okozhatnak a man-in-the-middle, és egyéb DNS ellen irányuló támadások.

- Fontos szempont egy vállalat, szervezet, vagy akár a magánemberek esetében, hogy egy módszer amit alkalmazni szeretnének (vagy alkalmazni kényszerülnek) milyen költségekkel jár.

  A kimenő e-mail szerverek (outbound email servers) esetében a Sender ID Framework alkalmazása sok többletmunkát, illetve költséget nem okoz, hiszen mindössze a DNS rekordot kell módosítaniuk. A DomainKeys-hez szükséges nyilvános kulcsú titkosításnál alkalmazott kulcs pár (vagy kulcs párok) alkalmazása, kezelése viszont felvet néhány kérdést:

  - § Mindenképpen meg kell oldani a titkos kulcs megfelelő tárolását, hiszen a DomainKeys módszer csak addig nyújt valamiféle biztonságot, amíg a titkos kulcs titkosságát megőrzik. Ha kompromittálódik a titkos kulcs, akkor mindenképpen azonnali cserére van szükség, vagyis fellépnek a szokásos kulcskezeléssel kapcsolatos problémák.
  - § Ha egy ISP, vagy domain-tulajdonos több nyilvános / titkos kulcs párt is használ, akkor az előző probléma fokozottan jelentkezik.

A bejövő e-mail szerverek (inbound email servers) szoftverei változtatást igényelnek. Támogatniuk kell a Sender ID teszt elvégzését, illetve a nyilvános kulcsú kriptográfiai műveletek (digitális aláírás) ellenőrzését. Ezen kívül a kliens szoftvereket is érdemes módosítani, hogy tájékoztatni lehessen a felhasználót a Sender ID teszt illetve DomainKeys ellenőrzés eredményéről.

Az e-mail továbbító szerverek, illetve egyéb „közbülső” szerverek esetében szintén az előzőekhez hasonló szoftverváltoztatásokra van szükség.

Ryan Hamlin (general manager of Microsoft’s Safety Technology and Strategy Group) a már említett nyilatkozatában utalt arra, hogy számos MTA, illetve ISP már elvégezte ezeket a kívánt módosításokat.

A DomainKeys esetében a Yahoo! már fejleszt egy referencia implementációt, melyet állításuk szerint számos MTA-ba (mint például a qmail-be) be lehet majd illeszteni. Ennek egy alpha verziója már el is érhető. Ezeken felül a Yahoo! együttműködik a Sendmail-lel, hogy abban is implementálják az eljárást (lényeges információ, hogy ez mind a kereskedelemi, mind a freeware verziókra igaz). Egy nyílt forráskódú implementációt a Sendmail már tesztelésre nyilvánosságra is hozott.

Nagyon meghatározó lehet az elterjeszthetőségben, hogy milyen biztonságot nyújtó kulcsokkal dolgozik a módszer. A megfelelő kulcsméret megválasztása egy értelmes kompromisszumot kell hogy jelentsen a költség, a teljesítmény és a biztonság eltérő követelményei között. Ennek következtében a javaslat még nem tartalmaz konkrét értékeket. (2048 bitnél hosszabb kulcsokat már nem javasolnak, hiszen egy 512 byte-os DNS UDP válaszba ennyi fér bele.)

Ezzel kapcsolatban jelentkezik a DomainKeys, illetve ezzel együtt a Sender ID-vel kombinált változat elterjeszthetőségének egy esetleges korlátja. Köztudott, hogy a nyilvános kulcsú kriptográfiai algoritmusok számítási igénye relatíve nagy.

Jelen esetben ez most azt jelenti, hogy először egy hash értéket kell számolni az e-mailre, majd ezt követi az RSA számítása. Ez a többi, eddig is alkalmazott ellenőrzés (vírus, spam) elvégzése mellett jelentős többletmunkát igényel.

A fenti probléma nagy mennyiségű levél esetén (mint például egy freemail, vagy hotmail esetén) már komoly gondokat okozhat.

A gyakorlatban 1024 bitnél hosszabb kulcsok használatát nem javasolják a DomainKeys kidolgozói sem.

4. A levonható következtetések:

Az eddigi áttekintés alapján lehetőség nyílik arra, hogy megítéljük Magyarországon mennyire lehetnek hatásosak ezek a törekvések.

Az újjáalkotott Sender ID Framework, Yahoo’s DomainKeys módszerek a domain spoofing ellen elméletileg megoldást jelentenek. Ez azonban csak akkor jelenthető ki, ha kellően elterjedtté válnak.

Az elterjedést nagymértékben befolyásolhatja, ha a Microsoft-nak sikerül elérnie, hogy az IETF szabványosítsa az eljárásukat. Amíg ez nem történik meg, addig nem fogják sokan választani a Sender ID-t. Ezt már önmagában az indokolja, hogy a módszer implementálásához még mindig

alá kell írni egy licenc-nyilatkozatot [3] a Microsoft felé, ami akármennyire is jelentéktelen dolognak tűnik, mégiscsak egy függést jelent a vállalattól (ami egyes szervezetek szempontjából akik implementálnák, döntő érv lehet). Itt a licenc kérdésével kapcsolatban érdemes tisztázni a legfőbb különbséget az SPF (Sender Policy Framework) és a Sender ID között. Az SPF GPL (General Public Licence) [7] alá tartozik, míg a Sender ID szoftverszabadalom. Az SPF licence egy konkrét megvalósításra (implementációra) vonatkozik, a Sender ID esetében azonban a működési elvet védték le.

A másik általunk gátló tényezőnek ítélt dolog az, hogy mind a Sender ID Framework, mind a Yahoo's DomainKeys módszerek még mindig csak a domain-t authentikálják, valamint eleve csak a domain spoofing (ezzel párhuzamosan természetesen a phishing) ellen nyújtanak védelmet. Vagyis attól, hogy mindenki összefog és sikerül elterjeszteni, kiépíteni ezt a módszert, még mindig ott marad a kéretlen reklámlevelek egy része.

- Egy vállalat, zárt domain esetén lehetőség nyílhat annak biztosítására, hogy arról az IP címhez tartozó gépről, amit a domain hitelesnek nyilvánít, tényleg csak az arra jogosult személyek küldjenek leveleket.
- Azon felhasználók esetén is, akik egy meghatározott ISP-n keresztül jutnak e-mail küldési lehetőséghez szigorításokkal ez még mindig megvalósítható lenne.

Tehát a domain spoofing megszűntetése mellett a további spammelés is korlátozható lenne, illetve lehetőség nyílhatna az esetleges elkövetők pontos azonosítására, megfelelő intézkedésekre.

A problémát továbbra is az okozza, hogy több szolgáltató is lehetőséget kínál ingyenes e-mail küldésre, amivel nagyon könnyen vissza lehet élni. A Sender ID-t már egyszerűen azzal ki lehet játszani, hogy valaki igényel egy ingyenes szolgáltatótól egy e-mail címet. Nincsen rászorítva arra, hogy a tényleges adatait adja meg, így attól sem kell tartania a felhasználónak, hogy később bárki is felelősségre vonná. Ha viszont már regisztrálta magát, onnét kezdve ő is hitelesítettnek minősül és elkezdheti küldözgetni a kéretlen reklámleveleket. Habár domain spoofing-ra már nem nyílhat lehetősége, a hálózatot mégis tovább terhelné a többi fajta spam. Ebben az esetben még mindig megmarad az a védelmi intézkedés, hogy az ingyenes szolgáltatók korlátozzák, hogy egy adott időszakban a felhasználó mennyi e-mailt küldhet el. Ekkor viszont a támadó többször is regisztráltathatja magát és ezzel már ki is játszotta ezt a fajta korlátozást.

Ha a DomainKeys-t vizsgáljuk, a helyzet hasonló. A privát / publikus kulcs pár tulajdonosa a kimenő szerver szolgáltató. Ennél fogva regisztráció után akárkit hitelesít a privát kulccsal. Ráadásul a megnövekedett számítási igények miatt igen könnyen DoS támadást indíthat valaki egy SMTP szerver ellen.

Valamelyest az oldaná meg a problémát (és a domain spoofing mellett itt a többi fajta spam küldését is értem), ha minden felhasználó rendelkezne saját nyilvános / privát kulcsokkal. Ez azonban a mai viszonyok szerint lehetetlen követelmény, hiszen ehhez már szükség lenne a PKI alkalmazására, amely nagyon költséges, valamint a jelenlegi DomainKeys javaslat nem is alkalmazná a CA-kat, emiatt ezt is módosítani kellene.

5. Végső összegzés:

Összegzésként azt lehet elmondani, hogy az SPF, ami már elterjedtebbnek mondható, ugyanúgy kombinálható lehetne a DomainKeys-vel mint a Sender ID Framework. Az eddig felsorolt érvek miatt, valamint a két módszer (Sender ID Framework és Sender Policy Framework) közötti kompatibilitási kérdéseket vizsgálva, az SPF vonzóbb előnyöket nyújthat a leendő implementálók számára. Természetesen ebben az esetben is szükség lenne DNSSEC alkalmazására is.

6. Hivatkozások:

[1]: *Sender ID: Authenticating E-mail; draft-lyon-senderid-core-00.txt October 2004*

[2]: *Sender ID Framework – Deployment Overview; Microsoft Corporation August 25, 2004*

[3]: *Sender ID Patent License Agreement*

[4]: *Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys); Yahoo! Inc August 2004*

[5]: *Microsoft – Information for Journalists - Q&A: Sender ID Framework Proposal Provides*

Foundation for Fight Against Malicious Spam; REDMOND, Wash. -- Oct. 25, 2004 [6]: *DomainKeys: Proving and Protecting Email Sender Identity; Yahoo! Inc 2005*
[7]: *GNU General Public License*