A Magyarországon alkalmazott spamszűrési módszerek és a Sender ID

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.
A 2004. júniusában tartott E-mail Technology Conference rendezvényen Vint Cerf (aki a TCP/IP kidolgozásában is részt vett) azt javasolta, hogy a legfontosabb lépés a spamek megállítására a küldők azonosságának megállapítása lenne.
Nagyjából ezt a vezérelvet követi a Sender ID Framework, melyet az e-mail domain spoofing visszaszorítására, illetve magasabb szintű biztonságot nyújtó szolgáltatások biztosítására 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 egész eljárás alapját egy döntési probléma adja, amelyet így foglalhatnánk össze: adva van egy e-mail és egy IP cím, ahonnan ezt az üzenetet elküldték, a kérdés pedig az, hogy az adott IP címhez tartozó SMTP kliens jogosult-e elküldeni az üzenetet?
A probléma általában SMTP szerverek esetén merül fel, amelyeknek el kell dönteniük, hogy elfogadják-e a bejövő e-mailt. Ennek a kérdésnek a megválaszolására dolgozták ki a Sender ID Framework-t. Az eljárás egyszerű lépésekből áll:

1. Az e-mail küldők nyilvánosságra hozzák kimenő e-mail szerverük IP címét a Sender ID specifikációban rögzítettek 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, amely 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 e-mailt 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 azonban egyre több probléma merült fel a megvalósíthatósággal, elterjeszthetőséggel kapcsolatban (többek között a licensz kérdése, iparági támogatás hiánya, kompatibilitási problémák). Éppen ezért akik szeretnének valamilyen spamelleni módszert alkalmazni, egyre nehezebben tudják eldönteni, hogy tényleg érdemes-e a Sender ID-t használni.
Az előadásomban egy átfogó képet szeretnék adni a jelenleg alkalmazott trendekből. Statisztikákat használva először is azt megmutatni, hogy ma Magyarországon a szervereken mely spamelleni módszereket alkalmazzák.
Miután láthatóvá válik a konkrét elterjedtség, a továbbiakban az egyes eljárásokat hasonlítom össze a használhatóság, a további terjeszthetőség lehetőségének szempontjából. Minden módszer esetében kiemelem, hogy a mai magyarországi implementációk miben különböznek egymástól. Vagyis nem a Sender ID működését, problémáit szeretném ismertetni, hiszen erről már számos összefoglalót hallhattunk.
Végül az eddig elmondottak alapján lehetőség nyílik egy végső konklúzióra is, hogy a többi módszer ismeretében vajon megállja-e a helyét a Sender ID.