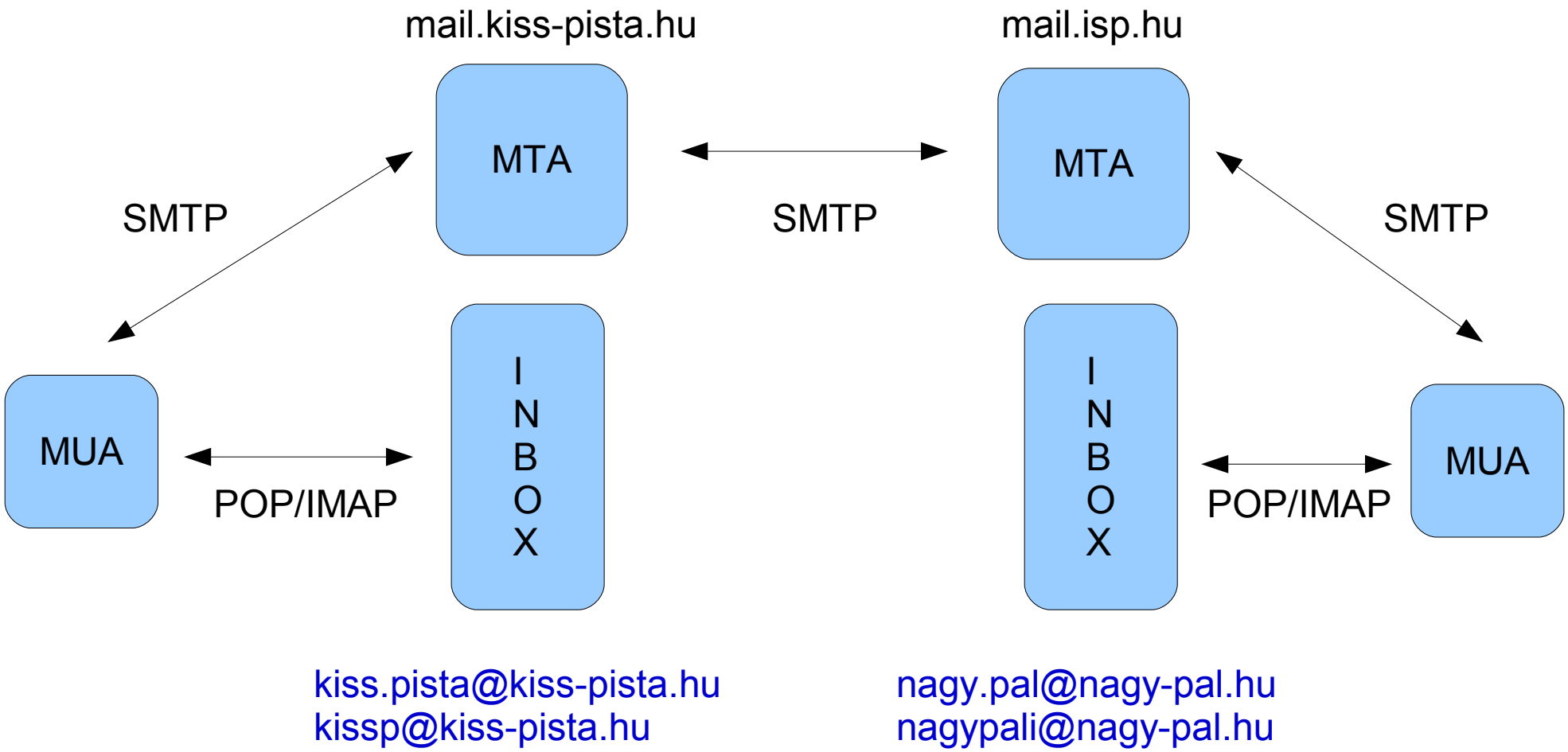
SPF és spamszűrés

Kadlecsik József
KFKI RMKI
<kadlec@sunserv.kfki.hu>

Tartalom

- Az elektronikus levelezés működés
- Spammer technikák
- Mi az SPF és miért okoz több kárt, mint hasznot?

Elektronikus levelezés



Az SMTP és a DNS

- @domain-part: MX vagy A (AAAA) rekord
- MX rekord: súly és A rekord (**nem** CNAME):

  % `dig -t mx domain-part`
- Backup MX rekord
- Wildcard A/MX rekord
  - 2003.09.15: Verisign SiteFinder: .com. .net
    - hibadetektálási nehézségek
    - potenciális E-mail cím gyűjtés
    - hamisított (nem létező) E-mail címek valódinak tűnnek

SMTP

- store and forward
- Levél (nyomtalanul) nem veszhet el:
  - bounce
  - double-bounce
- A '.'-ra válaszul adott '250 Ok' üzenettel a levél kezelésének gondját a fogadó szerver veszi át.
- A '.'-ra a válasz nem jöhet “túl soká”:
  - levél-duplikálás
- demo

SMTP és E-mail fejléc

- SMTP:

```
MAIL FROM: <joe@somewhere.com>
RCPT TO: <target@mail.host>
```

- E-mail fejléc:

```
From: George.W.Bush@whitehouse.gov
To: Condoleezza.Rice@whitehouse.gov

Return-Path: <joe@somewhere.com>
X-Original-To: <target@mail.host>
```

Spam formák

- Kéretlen E-mail
  - illegális, fél-legális kereskedelem
  - pornó
  - pénzügyi beugratások, csalás, phising
- Vírusos levelek és értesítések
- Joe-jobbing és backscatter

Spammerek céljai

- Nagy tömegű E-mail küldése:
  - open relay-ek
  - lyukas CGI/PHP script-ek (formmail)
  - open proxy (zombi) gépek – vírusok
  - offshore ISP-k: Kína, Dél-Korea, Indonézia, Malajzia, volt Szovjet államok, Dél-Amerika, stb.
  - *pink contract*: neves ISP mögött felárért

Spammerek céljai, folyt. I.

- Rejtőzködés, nyomok elfedése
  - host ISP mail szerverének elkerülése: direct-to-MX szoftverek
  - hamisított E-mail fejlécek (Received, Message-ID, stb.)
  - hamisított To: és From: E-mail fejlécek

Spammer trükkök

- Tartalomszűrők kikerülése:
  - Kódolt/valódi mögé rejtett URL-e; MIME, URL, HTML kódolások alkalmazása
  - Random karakterek, szövegrészek beillesztése: böngésző a felhasználó felé nem (észrevehetően) mutatja (MIME, HTML, CSS trükkök), tartalomszűrőt félrevezeti
  - Szándékosan hibás írásmód
  - Hibás, nem létező HTML tag-ek

Példák: The Spammers' Compendium,

http://www.jgc.org/tsc/

Spammer trükkök, folyt.

- DNS játékok:
  - eldobható DNS nevek spam küldésére; domain kiting
  - különböző IP blokkból több IP cím a webszervernek; portálok és társcégek
  - az IP címek (akár több tucatnyi) gyors rotálása
  - DNS kikapcsolása, miután a DNS cache-k megtanulhatták
  - DNS válasz késleltetése/letiltása az automatizált spam-keresők számára (SpamCop)
  - wildcard DNS rekordok

Védekezési lehetőségek

- SMTP szintű védelem:
  - before-queue
- Tartalomszűrés
  - before-queue: potenciális problémák
  - atfer-queue
- Előnyök és hátrányok!

SPF

- Sender Policy Framework (Sender Permitted From)
- RFC-4408
- Mely SMTP szerverek küldhetnek E-mail-t az adott E-mail cím(tartomány)al mint feladóval
  - MAIL FROM (Return-Path)
- DNS TXT rekord
  - SPF rekord

DNS rekord

example.com TXT

“v=spf1 +mx a:colo.example.com/28 -all”

smtp-out.example.com TXT

“v=spf1 a -all”

- a, mx, ptr, ip4, ip6, exists, include, all
- macro támogatás
- pass (+), fail (-), softfail (~), neutral (?), none
- Méretkorlátok: 450 byte (UDP)

Problémák: I.

- A DNS TXT rekord nem az SPF céljaira készült
  - TXT rekord struktúra nélküli
  - DNS SPF rekord: RFC-4408 az SPF mellett előírja a TXT rekord lekérdezését is

Problémák: II.

- SPF nem kompatibilis a már létező SMTP architektúrával és annak forward/alias funckionalitásával (RFC-1123)

SMTP1 ---> SMTP2 ---> SMTP3

S: a@foo forward to S: a@foo

R: x@bar y@fie R: y@fie

  - SRS (Sender Rewriting Scheme) nem megoldás

Problémák III.

- Az SMTP fallback MX funkcionalitásával nem kompatibilis (RFC-974, RFC-2821)
  - dobjuk ki a fallback MX rekordokat
  - szeparáljuk az SMTP relay funkcionalitást, kezelt mail domain-enként

Problémák IV.

- A felhasználókat egyrész még jobban kiszolgáltatja az ISP-nek:
  - más ISP-t levelezésre nem használhat; roaming
- Megköti az ISP-t:
  - kötelező SMTP szerver üzemeltetés
  - SMTP Auth, VPN, webmail
  - *egy mindenkiért, mindenki egyért*

Problémák V.

- DNS lekérdezések eredménye cache-be kerül
  - TTL
  - SPF rekord cseréjét tervezni kell

Problémák VI.

- Az SPF nem megoldás a spam ellen
  - zombi gépek az SPF-nek megfelelő SMTP szerveren keresztül küldik a leveleiket – mail quota?
  - spammereket semmi sem akadályozza meg SPF rekordok hirdetésében

Problémák VII.

- 2003. 08. 15: Verisign .com és .net wildcard A record (SiteFinder)
  - Ugyanez megtörténhet az SPF rekorddal is!

Összefoglalás

- Az SPF nem megoldás és nem csökkenti a spam mennyiségét
- Tovább erodálja a már amúgy is a működőképesség határáig feszített SMTP működését

Ne használjuk az SPF-et.