HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

SPAM

CCERT-PUBDOC-2005-02-108

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

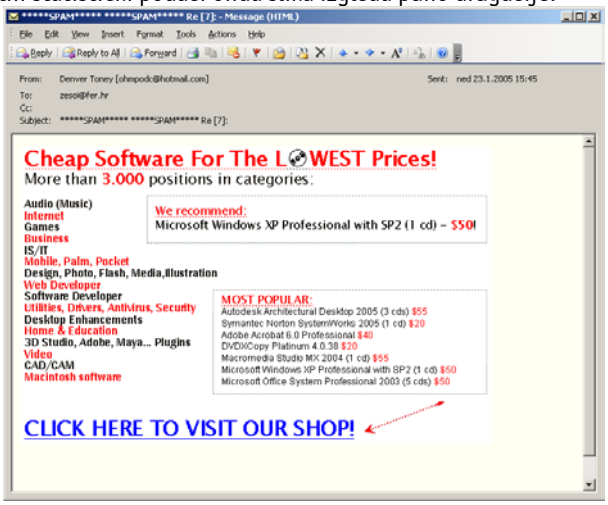
Sadržaj

1. Uvod

Spam, odnosno neželjena elektronička pošta problem je koji već dugi niz godina brine gotovo sve korisnike Interneta. Bez obzira radi li se o krajnjim korisnicima, velikim tvrtkama ili davateljima Internet usluga, problem *spam*a osim što uznemirava korisnike također za sobom povlači i ogromne financijske gubitke. Usprkos brojnim pokušajima suzbijanja *spama* korištenjem različitih alata, tehnologija, te primjenom zakonskih regulativa, neželjena elektronička pošta još uvijek je neriješen problem gotovo svih informacijskih sustava. Slobodno se može reći da je velik broj korisnika čak *spam* prihvatilo kao neizbježan problem na koji se ne može puno utjecati i koji treba kao takav prihvatiti.
Dokument daje pregled problema vezanih uz neželjenu elektroničku poštu, osnovne tipove i karakteristike *spam* poruka te mogućnosti zaštite koje korisnici i sistem administratori mogu iskoristiti u svrhu zaštite od *spam*a. Također je dan pregled zakonske regulative na ovom području te opis nekih od novijih tehnologija koje bi trebale pomoći u suzbijanju *spam*a.

2. Općenito o *spam*u

Osim uznemirujućeg karaktera kojeg neželjena elektronička pošta ostavlja na krajnjeg korisnika, problemi *spam*a puno su širi. Neželjene poruke elektroničke pošte mogu utjecati na narušavanje ugleda i integriteta tvrtki i pojedinaca, zatim uzrokovati iskorištavanje računalnih resursa u vidu procesorskog vremena, prostora na tvrdom disku, mrežne propusnosti i sl. Vrijeme i energija koju korisnici troše za svakodnevno pregledavanje i brisanje *spam* poruka također utječe i na pad njihove produktivnosti, a moraju se uzeti u obzir i dodatni troškovi vezani uz rješenja kojima se korisnici nastoje boriti protiv ovog problema. Možda na prvi pogled ovi problemi nisu toliko očiti, no ukoliko se u obzir uzmu relevantni statistički podaci onda slika izgleda puno drugačije.



Slika 1. Primjer spam poruke

Statistike pokazuju da dnevno Internetom kruži oko 30 milijardi poruka elektroničke pošte. Od toga na *spam* otpada između 40-60% (ovisno o analizama), što znači oko 15-18 milijardi poruka. Ukoliko se taj broj pomnoži s vremenom koje je u prosjeku potrebno korisniku da prepozna i obriše *spam* poruku (procjene su da ovo vrijeme u prosjeku iznosi od 4-5 sekundi) te brojem dana u godini, onda dolazimo do konačnog rezultata koji jasno ukazuje na ozbiljnost problema. Prema posljednjim procjenama u SAD-u troškovi se kreću od 250 milijuna dolara za obične korisnike i do 9 milijardi dolara za tvrtke što su ogromni financijski gubici. Iako je problem djelomice moguće ublažiti korištenjem specijaliziranih *antispam* alata i servisa, čija kvaliteta i učinkovitost varira od proizvoda do proizvoda, *spam* je problem protiv kojeg se još uvijek bore gotovo svi korisnici Interneta.
Interesi *spam* industrije očito su veliki, budući da se usprkos brojnim zakonskim i tehničkim mjerama broj *spam* poruka ne smanjuje. U zadnjih nekoliko godina *spam* industrija znatno je napredovala i proširila se po cijelom svijetu. Iako je Amerika još uvijek na prvom mjestu, ostale zemlje kao što su J. Koreja, Kina, Brazil vrlo su blizu.

Spam industrija generalno se može podijeliti na tri usko povezana dijela. Prvi dio čine skupljači adresa (engl. *list makers*) koji svakodnevno pretražuju Internet u potrazi za novim adresama koje će se koristiti za slanje *spam* poruka. U ovu svrhu koriste se vrlo sofisticirani programi koji naprednim tehnikama pretražuju različite resurse na Internetu (Web stranice, news grupe i sl.) te pohranjuju pronađene mail adrese. Ove adrese kasnije se prodaju zainteresiranim osobama, najčešće samim *spammerima* koji ih koriste za masovno slanje poruka.
Sljedeći važan element čine sami *spammeri*, odnosno osobe koje šalju *spam* poruke. Ovaj aspekt *spam* industrije znatno je napredovao od prvih početaka *spam*-a, budući da danas postoje velike organizacije, pa čak i davatelji Internet usluga, koji kao uslugu nude upravo slanje *spam* poruka. Za razliku od legitimnih davatelja Internet usluga koji vode računa da se sa njihovih adresa ne šalju spam poruke, ovakve organizacije registrirane su upravo kako bi se *spammerima* omogućilo masovno slanje neželjene elektroničke pošte. Za slanje poruka najčešće se koriste tzv. *mass mailing* programi koji identičnu poruku šalju na velik broj adresa, pri čemu se koriste brojne tehnike lažiranja poruka kojima se pokušava otežati identifikacija izvora pošiljatelja.
Posljednji važan element su osobe koje ovim putem pokušavaju ostvariti vlastite interese najčešće u obliku financijske zarade. Karakter i sadržaj *spam* poruke ovisit će o interesu *spammera*, no najčešće se radi o porukama reklamnog karaktera kojima se korisniku nudi određeni proizvod ili usluga.

2.1. Vrste *spama*

Ovisno o izgledu poruke, načinu njenog slanja i tipu, *spam* poruke mogu se podijeliti u nekoliko kategorija. Najzatupljenija kategorija su *spam* poruke komercijalnog tipa (*engl. unsolicited commercial e-mail ili UCE*).
U nastavku su opisane neke od tipičnih kategorija *spam* poruka, zajedno s njihovim osnovnim značajkama.

- **Email *spam***:
  - Neželjena komercijalna elektronička pošta (engl. *unsolicited commercial e-mail ili UCE*) podrazumijeva poruke elektroničke pošte koje reklamiraju određeni proizvod ili uslugu, a da sam korisnik to nije zatražio. Ovakav tip poruka još se naziva i *junk e-mail*.
  - Neželjena *bulk* elektronička pošta (*engl. unsolicited bulk e-mail ili UBE*) odnosi se na poruke elektroničke pošte koje su iz određenog interesa poslane tisućama, pa čak i milijunima korisnika. Najčešći karakteri poruka ovog tipa su politička lobiranja i uznemiravanje korisnika.
  - *Make money fast ili MMF* poruke, najčešće u obliku lančanih pisama ili piramidnog marketinga, su tip *spam* poruka koje korisnicima nude brzu i laku zaradu ukoliko na određenu adresu pošalju određenu svotu novaca. Većina poruka od korisnika zahtjeva da poruku dalje proslijede drugim korisnicima. Iako vrlo primitivne i očite, ovakav tip poruka još uvijek zavarava velik broj korisnika, pogotovo onih manje iskusnih.
  - Napadi na reputaciju (*engl.reputation attacks*) su lažirane poruke elektroničke pošte poslane u ime neke druge osobe ili organizacije. Osnovna uloga im je ugrožavanje reputacije i kredibiliteta subjekta u čije se ime poruka šalje.
- **Usenet spam**:
  - *Excessive multi-posting (EMP)* odnosi se na situaciju kada se identična news poruka individualno pošalje na velik broj *newsgrupa*. Svaka kopija vijesti ima različiti identifikacijski broj (engl. *Message-ID*) i tipično se pojavljuje u različitim newsgrupama. Na taj način svaka se poruka šalje na sva računala povezana na Usenet poslužitelje.
  - *Excessive cross-posting (ECP) spam* odnosi se na vijesti koje su poslane (engl. *cross-posted*) na velik broj newsgrupa. Vijest je poslana na više *newsgrupa* sadržanih u zaglavlju poruke.
  - *Spew* se događa kada neispravno podešeni *news* program istu poruku pošalju na velik broj *newsgrupa*. Postavljanje vijesti različite teme (*engl. off-topic postings*) od one za koju je namijenjena određena *newsgrupa*. Npr. članak o sportu nije prihvatljiv u grupi koja se bavi temama kao što su računala, automobilizam i sl.

- Binarne poruke (engl. *binaries*) su poruke koje sadrže binarno enkodirane datoteke, kao što su slike, muzika, video itd. Neprihvatljive su na grupama koje nisu binarne.

2.2. Tehnike slanja *spama*

Za slanje *spam* poruka *spammeri* često koriste specijalne alate (*engl. bulk mailers*) koje najčešće i sami razvijaju. Ovakvi alati sadrže niz različitih funkcionalnosti prilagođenih slanju *spam* poruka kao što su lažiranje zaglavlja poruka elektroničke pošte, dodavanje elemenata za zaobilaženje *antispam* filtara, prikrivanje izvora, automatizirano pronalaženje i prikupljanje *spam* poruka i sl. Ti alati neprestano se razvijaju u skladu s novim potrebama i zahtjevima *spammera*.
Budući da većina legitimnih davatelja Internet usluga ne tolerira slanje *spam* poruka preko njihovih mail poslužitelja, *spammeri* su morali pronaći nove mehanizme za slanje poruka. U tom smislu najpoznatije su tri metode koje *spammerima* omogućuju slanje neželjenih poruka elektroničke pošte, a da pritom u velikoj mjeri ostanu anonimni:

- **Open relay** poslužitelji su nezaštićeni MX (engl. *mail exchanger*) poslužitelji koji omogućuju slanje poruka elektroničke pošte bilo kome na Internetu. Ovakvi mail poslužitelji danas su neprihvatljivi sa stanovišta sigurnosti, budući da *spammerima* omogućuju vrlo jednostavno slanje poruka te prikrivanje njenog izvora. Svaki mail poslužitelj morao bi omogućavati slanje poruka samo autoriziranim korisnicima, što je najčešće ograničeno na internu računalnu mrežu organizacije. Ukoliko je potrebno dozvoliti slanje poruka s nepoznatih adresa (kao što je slučaj npr. sa modemskim ulazima) koriste se servisi za SMTP autentikaciju kao što je SMTP AUTH.
- **Web site mail-form hijacking.** Za slanje poruka *spammeri* vrlo često iskorištavaju i nesigurne skripte za slanje poruka koje su postavljenje na nezaštićenim Web poslužiteljima. Putem specijalnih Web formi namijenjenih slanju poruka elektroničke pošte, *spammeri* mogu vrlo jednostavno automatizirati postupak slanja poruka, a da pritom ostanu anonimni.
- **Open proxy.** S obzirom na ulogu i način rada, nezaštićeni proxy poslužitelji gotovo su idealni za slanje *spam* poruka. Korištenjem otvorenih proxy poslužitelja *spammeri* mogu vrlo jednostavno inicirati konekciju prema bilo kojem računalu na Internetu, a da se pritom kao izvor poruke vidi adresa proxy poslužitelja. Kao otvoreni proxy poslužitelji mogu se koristiti pogrešno podešeni programski paketi kao što su SQUID i njemu slični, a sve su češći primjeri gdje neovlašteni korisnici kompromitiraju osobna računala korisnika i na njima pokreću specijalne proxy programe koje kasnije koriste za slanje *spam* poruka. Sami korisnici računala vrlo često nisu ni svjesni da se njihovo računalo koristi u neovlaštene svrhe, što *spammerima* omogućuje neometano slanje poruka u dužem vremenskom periodu. Kompromitirana računala koja se koriste za slanje *spama* nazivaju se zombi računala (engl. *zombie*).

Osim upravo opisanih tehnika za masovno slanje poruka i prikrivanje njihovog izvora, *spam* poruke redovito sadrže brojne elemente kojima se želi zaobići *antispam* filtre. U nastavku su navedene neke od popularnijih tehnika koje *spammeri* koriste za zaobilaženje *antispam* filtara:

- Namjerno pogrešno napisane riječi (umjesto izraza viagra koriste se izrazi kao što su v|@gr@ ili \ /|agra). Budući da se većina jednostavnih *antispam* filtara bazira na pretraživanju ključnih riječi u porukama elektroničke pošte, na ovaj način moguće je vrlo jednostavno zaobići njihove provjere.
- Ubacivanje HTML oznaka unutar poznatih riječi (npr. vigra). Kada klijent elektroničke pošte interpretira tekst poruke, on interpretira i sadržane HTML oznake (ukoliko je omogućen pregled poruka u HTML obliku) kako bi se poruka prikazala na ispravan način. U tom slučaju korisniku se riječ prikazuje u željenom obliku, dok će, zbog ubačenih HTML oznaka filtar biti zaobiđen. Vrlo često se u poruke ubacuju i nepostojeće HTML oznake koje će e-mail klijent u tom slučaju jednostavno odbaciti i korisniku prikazati željeni tekst, dok će filtar biti zaobiđen.
- Dodavanje specijalno formiranog teksta na kraj poruke elektroničke pošte s ciljem zavaravanja *antispam* filtara. Ovaj tekst vrlo se često prikazuje u istoj boji kao i podloga poruke, kako bi bio nevidljiv za primatelja poruke.
- Korištenje različitih načina kodiranja e-mail poruke.

2.3. Tehnike prikupljanja adresa elektroničke pošte

Jedno od osnovnih obilježja *spam* poruka je to da se one šalju na iznimno velik broj korisničkih adresa. Na taj način povećava se vjerojatnost da će neki od korisnika pročitati poruku i postupiti u skladu s sadržajem koji je u njoj naveden. Samim time moguće je zaključiti da je jedan od temeljnih koraka *spammera* upravo prikupljanje adresa elektroničke pošte na koje će slati svoje poruke.
U nastavku poglavlja navedeni su neki od primjera kako *spammeri* dolaze do korisničkih adresa:

- Kupovinom gotovih lista s milijunima adresa elektroničke pošte za nekoliko desetaka američkih dolara (oko 20$). Cijene ovakvih lista mogu varirati ovisno o tome da li su navedene adrese provjerene kao važeće, ili se radi o adresama koje su prikupljene bez dodatnih provjera. Kupljene liste jednostavno je moguće uključiti u specijalizirane programe koji će poruku poslati na navedene adrese u vrlo kratkom periodu.
- Korištenjem tzv. *e-mail extractors* programa koji pretražuju Internet tražeći adrese elektroničke pošte na Web stranicama, forumima, *newsgrupama* i drugim sličnim Internet servisima. Prosječni programi ovog tipa mogu izvući i do 15.000 adresa u jednom satu. Kako bi se onemogućio rad ovakvih programa, na brojnim Web stranicama počele su se primjenjivati različite metode kojima se adrese elektroničke pošte prikazuju u specifičnom formatu neprepoznatljivom za ovakve programe.
- Ručnim pretraživanjem Interneta i prikupljanjem adresa elektroničke pošte. Iako prilično spor proces u usporedbi s drugim metodama, sve se češće primjenjuje s obzirom da velik broj stranica koristi tehnike koje onemogućuju automatsko prikupljanje adresa.
- Korištenjem tzv. *newsgroup harvesters* programa koji automatski prikupljaju adrese s *newsgrupa*. Takav program može sakupiti desetke tisuća adresa u vrlo kratkom vremenu.
- Postavljanjem različitih Internet servisa koji od korisnika zahtijevaju ostavljanje adrese elektroničke pošte.
- Krađom gotovih lista adresa elektroničke pošte od davatelja Internet usluga.
- Korištenjem specijaliziranih programa koji korištenjem *brute-force* i *dictionary* tehnika pokušavaju pogoditi valjane adrese na određenoj domeni. Generiranjem slučajnih adresa koristeći uobičajena imena, pojmove i znakove, moguće je prikupiti prilično velik broj adresa za određenu domenu. Kako bi se pojedina adresa proglasila valjanom, od korisnika se očekuje odgovor na poslanu poruku. Primjer korištenja ove tehnike su generiranje adresa tipa info@example.com, uprava@example.com, mmarko@example.com, pperic@example.com i sl., a moguće je i korištenje čistih *brute-force* tehnika a@example.com, ab@example.com, abc@example.com itd. Ovakvi napadi mogu biti vrlo problematični za sistem administratore mail poslužitelja budući da se generira velik broj poruka o neuspjeloj isporuci (*nondelivery receipts* –NDR).

3. Analiza zaglavlja poruke elektroničke pošte

Prilikom slanja *spam* poruka *spammeri* koriste brojne tehnike lažiranja poruka elektroničke pošte, kako bi prikrili stvarni izvor od kuda su poslane. Osim **From** polja poruke, koje opisuje njenog pošiljatelja, najčešće se lažiraju i **Received** polja kako bi se prikrio stvarni tijek komunikacije između izvornog i ciljnog SMTP poslužitelja. **Recieved** polja dodaju se od strane svakog mail poslužitelja na putu od pošiljatelja do primatelja poruke te je njihovom analizom moguće utvrditi izvor od kuda je poruka poslana (pritom se misli na IP adresu mail poslužitelja ili računala s kojeg je poruka poslana, a ne na identitet korisnika).
Upravo zato *spammeri* vrlo često u zaglavlje poruke dodaju lažirana **Recieved** polja kako bi se korisnike navelo na krivi put prilikom pokušaja identifikacije izvora *spam* poruke. S istim ciljem se za slanje poruka koriste i nezaštićeni *open relay* i *open proxy* poslužitelji koji u zaglavlje poruke dodaju vlastite adrese kao izvor poruke. Iz svega navedenog moguće je zaključiti kako je lažiranje poruka elektroničke pošte vrlo važan segment u postupku generiranja i slanja *spam* poruka. Kada se ne bi primjenjivale brojne tehnike lažiranja poruka i prikrivanja njihovog izvora, pošiljatelje *spam*-a bilo bi mnogo jednostavnije identificirati i njihove bi se adrese mogle jednostavno unijeti na globalne crne liste (*engl. blacklist*) koje bi onemogućile daljnje slanje *spam*-a s tih poslužitelja.

Budući da trenutna specifikacija SMTP protokola ne sadrži sigurnosne kontrole koje bi spriječile lažiranje poruka, problem borbe protiv *spam*-a dodatno je otežan. Za preciznu identifikaciju izvora *spama* potrebno je dobro razumjeti strukturu zaglavlja poruke elektroničke pošte i znati kako ju interpretirati. Kada se govori o analizi *spam* poruka najvažnije je ispravno tumačenje **Recieved** zaglavlja te ispravno prepoznavanje elemenata koji su namjerno umetnuti u poruku s ciljem zavaravanja korisnika. **Recieved** polja sadrže važne informacije o mail poslužiteljima kroz koje je poruka prošla, vremenima slanja poruka i sl., te su kao takva najznačajniji element u postupku identifikacije izvora poruke. Detaljnije informacije o zaglavljima i načinu slanja poruka elektroničke moguće je naći u RFC821 dokumentu na adresi http://www.faqs.org/rfcs/rfc821.html.
U nastavku je dan primjer zaglavlja *spam* poruke elektroničke pošte kako bi se na konkretnom primjeru pokazao značaj i smisao pojedinih elemenata zaglavlja poruke. Sadržaj poruke nije prikazan budući da nije važan u okviru ovog razmatranja.

```
Return-Path: <kevinwww@po.zzn.com>
From: kevinwww@po.zzn.com
Received: from h2.mail.home.com ([24.2.2.28]) by mail.rdc1.ab.home.com
          (InterMail v4.01.01.07 201-229-111-110) with ESMTP
          id
                    <19990728164203.WNNS19181.mail.rdc1.ab.home.com@h2.mail.
                    home.com>
          for <someuser@mail.ssdt1.sk.wave.home.com>;
          Wed, 28 Jul 1999 09:42:03 -0700
Received: from mx3-e.mail.home.com (mx3-e.mail.home.com [24.2.2.26])
       by h2.mail.home.com (8.9.3/8.9.0) with ESMTP id JAA29657
       for <someuser@home.com>; Wed, 28 Jul 1999 09:42:02 -0700 (PDT)
Received: from bftoemail10.bigfoot.com (bftoemail10.bigfoot.com
[208.156.39.200])
       by mx3-e.mail.home.com (8.9.1/8.9.1) with SMTP id JAA25058
       for <someuser@home.com>; Wed, 28 Jul 1999 09:42:02 -0700 (PDT)
Received: from relay.somedomain.com ([126.33.246.159])
          by bftoemail9.bigfoot.com (Bigfoot Toe Mail v1.0
          with message handle 990728_124133_6_bftoemail9_smtp;
          Wed, 28 Jul 1999 12:41:33 -0500
          for someuser@bigfoot.com
Received: from knusun.kangnung.ac.kr ([202.30.48.2])
       by relay.somedomain.com (8.9.3/8.9.0) with ESMTP id FAA294657
       for <someuser@home.com>; Wed, 28 Jul 1999 09:41:22 -0700 (PDT)
Received: from chem.kangnung.ac.kr (chem.kangnung.ac.kr [203.255.218.45]
         by knusun.kangnung.ac.kr (8.8.8H1/8.6.9) with SMTP id BAA29317;
         Thu, 29 Jul 1999 01:41:58 +0900 (KST)
Received: from chem.kangnung.ac.kr by chem.kangnung.ac.kr (SMI-8.6/SMI-SVR4)
         id BAA03348; Thu, 29 Jul 1999 01:40:04 +0900
         Date: Thu, 29 Jul 1999 01:40:04 +0900
Message-Id: <199907281640.BAA03348@chem.kangnung.ac.kr >
Received: from localhost [127.0.0.1]) by mx.aol.com (8.8.8H1/8.6.9) with
SMTP id BAA935176; Wed, 28 Jul 1999 23:55:32 +0900 (KST)
To: kevinwww@po.zzn.com
Subject: Findout About Anyone Fast (499651)
X-UID: 1510
```

Važno je napomenuti da se zaglavlja u poruku ubacuju onim redom kako poruka prolazi kroz poslužitelje na Internetu. To znači da prva **Recieved** linija na vrhu zaglavlja označava posljednji poslužitelj koji je proslijedio poruku, i tako redom sve do izvora od kuda je poruka inicijalno poslana. Ovakva struktura zaglavlja poruke podrazumijeva da će se lažirana **Recieved** polja, umetnuta od strane *spammera,* nalaziti pri dnu zaglavlja poruke.
U nastavku slijedi objašnjenje pojedinih zaglavlja dane poruke:

```
Return-Path: <kevinwww@po.zzn.com>
From: kevinwww@po.zzn.com
```

Ove linije ubačene su od strane klijenta elektroničke pošte na osnovu onog što je pošiljatelj upisao kao izvorišnu adresu. Prilikom analize zaglavlja poruke, ova se polja mogu zanemariti budući da ih je vrlo lako lažirati.
Sljedeći dio zaglavlja označava prosljeđivanje poruke između mail poslužitelja unutar računalne mreže davatelja Internet usluga (engl. *internal handoff*). U ovom slučaju radi se o računalnoj mreži **home.com** domene.

```
Received: from h2.mail.home.com ([24.2.2.28]) by mail.rdc1.ab.home.com
```

```
          (InterMail v4.01.01.07 201-229-111-110) with ESMTP
          id
<19990728164203.WNNS19181.mail.rdc1.ab.home.com@h2.mail.home.com>
          for <someuser@mail.ssdt1.sk.wave.home.com>;
          Wed, 28 Jul 1999 09:42:03 -0700 (PDT)
```

U nastavku je dan detaljniji opis **Recieved** polja kako bi se korisniku olakšala analiza zaglavlja poruke elektroničke pošte.

Prvi dio zapisa označava ime, odnosno IP adresu poslužitelja od kojeg je poruka primljena.

```
from h2.mail.home.com ([24.2.2.28])
```

Slijedi adresa poslužitelja koji je poruku primio, zajedno sa nazivom i inačicom mail poslužitelja (InterMail v4.01.01.07 201-229-111-110) i oznakom protokola (ESMTP). Također je naveden i identifikacijski broj koji je mail poslužitelj interno dodijelio ovoj poruci, ali njegov značaj je isključivo lokalan na poslužitelju na kojem je broj pridjeljen. Ovaj broj najčešće koriste sistem administratori prilikom analize log zapisa u slučaju eventualnih problema.

```
by mail.rdc1.ab.home.com
          (InterMail v4.01.01.07 201-229-111-110) with ESMTP
          id
<19990728164203.WNNS19181.mail.rdc1.ab.home.com@h2.mail.home.com>
          for <someuser@mail.ssdt1.sk.wave.home.com>;
```

Unutar svakog **Recieved** polja nalazi se i točan datum kada je poruka obrađena s pripadajućom vremenskom zonom (u ovom slučaju *Pacific Daylight Time –PDT zona koja je 7 sati iza Greenwich Mean Time – GMT zone).*

```
Wed, 28 Jul 1999 09:42:03 -0700
```

Slijedeći zapis također opisuje komunikaciju između dva mail poslužitelja unutar `home.com` domene davatelja Internet usluga.

```
Received: from mx3-e.mail.home.com (mx3-e.mail.home.com [24.2.2.26])
       by h2.mail.home.com (8.9.3/8.9.0) with ESMTP id JAA29657
       for <someuser@home.com>; Wed, 28 Jul 1999 09:42:02 -0700 (PDT)
```

Za razliku od prethodnih **Recieved** polja koja su opisivala razmjenu poruka između poslužitelja unutar iste domene, slijedeći zapis opisuje razmjenu poruka elektroničke pošte između dva MX poslužitelja u različitim domenama. Poslužitelj `mx3-e.mail.home.com` primilo je poruku namijenjenu korisniku someuser@home.com od poslužitelja `bftoemail10.bigfoot.com`. Ovakvo prosljeđivanje poruka naziva se *relaying.*

```
Received: from bftoemail10.bigfoot.com (bftoemail10.bigfoot.com
[208.156.39.200])
       by mx3-e.mail.home.com (8.9.1/8.9.1) with SMTP id JAA25058
       for <someuser@home.com>; Wed, 28 Jul 1999 09:42:02 -0700 (PDT)
```

Sljedeće zaglavlje opisuje razmjenu poruka između poslužitelja `relay.somedomain.com` i `bftoemail9.bigfoot.com`.

```
Received: from relay.somedomain.com ([126.33.246.159])
          by bftoemail9.bigfoot.com (Bigfoot Toe Mail v1.0
          with message handle 990728_124133_6_bftoemail9_smtp;
          Wed, 28 Jul 1999 12:41:33 -0500
          for someuser@bigfoot.com
```

Budući da adresa primatelja poruke (someuser@bigfoot.com) odgovara imenu e-mail poslužitelja koji procesira poruku, može se zaključiti kako je `bftoemail9.bigfoot.com` legitimni mail poslužitelj zadužen za isporuku poruke na zadanu adresu.

Analizom sljedećeg zaglavlja moguće je zaključiti da je poslužitelj `relay.somedomain.com` *open relay*. Analizom svih zaglavlja poruke može se vidjeti da spomenuti mail poslužitelj ne pripada niti pošiljateljevoj niti primateljevoj računalnoj mreži što potvrđuje da se radi o *open mail relay* poslužitelju.

Poslužitelj `relay.somedomain.com` poruku je primio od poslužitelja `knusun.kangnung.ac.kr`, što upućuje da je poruka izvorno poslana s računala na računalnoj mreži `kangnung.ac.kr` domene.

```
Received: from knusun.kangnung.ac.kr ([202.30.48.2])
       by relay.somedomain.com (8.9.3/8.9.0) with ESMTP id FAA294657
       for <someuser@home.com>; Wed, 28 Jul 1999 09:41:22 -0700 (PDT)
```

Izvedeni zaključak dodatno potvrđuje sljedeća **Recieved** linija koja opisuje komunikaciju između mail poslužitelja na kangnung.ac.kr domeni.

```
Received: from chem.kangnung.ac.kr (chem.kangnung.ac.kr [203.255.218.45]) by
knusun.kangnung.ac.kr (8.8.8H1/8.6.9) with SMTP id BAA29317; Thu, 29 Jul
1999 01:41:58 +0900 (KST)
```

Iz istog zapisa također se može zaključiti da je poslužitelj `knusun.kangnung.ac.kr` odgovorno za slanje poruke elektroničke pošte prema ostatku Interneta.
Slijedeće zaglavlje prvo je koje je u poruku ubačeno nakon njenog slanja, te je stoga vrlo vjerojatno da će administratori poslužitelja `chem.kangnung.ac.kr` moći utvrditi tko je generirao poruku.

```
Received: from chem.kangnung.ac.kr by chem.kangnung.ac.kr (SMI-8.6/SMI-SVR4)
       id BAA03348; Thu, 29 Jul 1999 01:40:04 +0900
Date: Thu, 29 Jul 1999 01:40:04 +0900
Message-Id: <199907281640.BAA03348@chem.kangnung.ac.kr >
```

Posljednji **Recieved** zapis ubačen je od strane *spammera*, što je moguće zaključiti na temelju detaljnije analize adresa i naziva računala koja sudjeluju u komunikaciji.

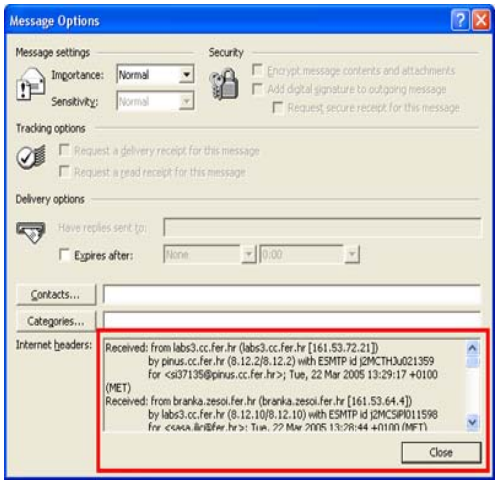
```
Date: Thu, 29 Jul 1999 01:40:04 +0900
Message-Id: <199907281640.BAA03348@chem.kangnung.ac.kr >
Received: from localhost [127.0.0.1]) by mx.aol.com (8.8.8H1/8.6.9) with
SMTP id BAA935176; Wed, 28 Jul 1999 23:55:32 +0900 (KST)
```

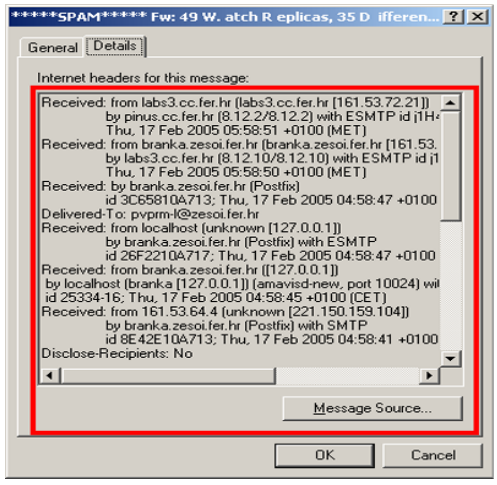
Računalo `mx.aol.com` nikako se ne uklapa u zaglavlje prikazane poruke, a i vremenska razlika između posljednja dva zapisa prevelika je za tipičnu SMTP komunikaciju između dva e-mail poslužitelja. Također, budući da KST vremenska zona pripada istočnoj Aziji, komunikacija s `aol.com` mail poslužiteljem dodatno je sumnjiva.
Nakon što je uspješno određena domena s koje je stigla *spam* poruka moguće je poslati službenu pritužbu administratorima kako bi se sankcionirale odgovorne osobe. Ukoliko adresa na koju je moguće poslati službenu prijavu incidenta nije poznata, istu je moguće pronaći na adresi http://www.abuse.net/lookup.phtml. Nakon što se upiše ime domene o kojoj je riječ, prikazat će se adresa na koju je moguće prijaviti detektirani incident. Najčešće adrese za ovakav tip prijave imaju oblik root@ime_domene, admin@ime_domene, webmaster@ime_domene, postmaster@ime_domene i sl.

3.1. Analiza zaglavlja poruka u email klijentima

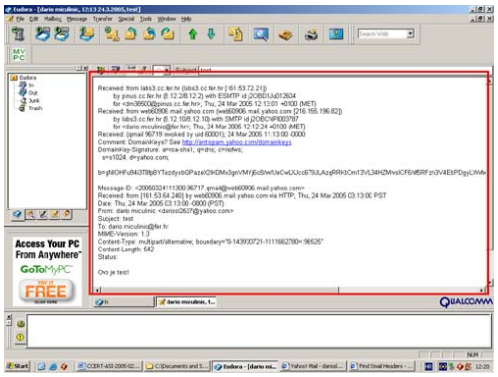
Gotovo svi klijenti elektroničke pošte imaju mogućnost prikaza zaglavlja poruke. Većina ih uobičajeno prikazuje samo **From**, **To** i **Subject** polja, tako da je potrebno uključiti posebnu opciju koja omogućuje prikaz cijelih zaglavlja.
U nastavku poglavlja navedene su osnovne upute kako vidjeti cijela zaglavlja poruke u nekim od poznatijih klijenata elektroničke pošte.

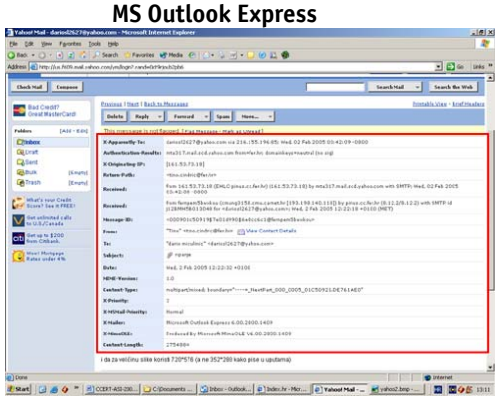
- Microsoft Outlook
  - kliknuti desnim gumbom na poruku
  - odabrati Options
- Microsoft Outlook Express
  - odabrati meni File
  - odabrati polje Properties
  - odabrati opciju Details
- Yahoo
  - odabrati **Full Headers.**
- Eudora
  - za otvaranje poruke dvaput kliknuti na poruku.
  - odabrati polje blah blah blah.





MS Outlook **MS Outlook Express**





Eudora **Yahoo Mail**

Dodatne upute za analizu zaglavlja poruke elektroničke pošte u različitim klijentima za pregledavanje elektroničke pošte moguće je pronaći na adresama http://www.jahitchcock.com/cyberstalked/header.htmili http://www.extreme-guides.com/sup/3/1/.

4. Zaštita od *spama*

Zaštitu od *spama* moguće je implementirati na nekoliko načina i obično je u praksi potrebno kombinirati više rješenja kako bi se postigla željena razina pouzdanosti. Također, i metode zaštite bitno će se razlikovati ovisno o tome da li se radi o osobnom računalu korisnika ili e-mail poslužitelju putem kojeg organizacija prima elektroničku poštu.

U nastavku poglavlja opisana su neka rješenja i alati kojima je osobna računala i e-mail poslužitelje moguće zaštititi od *spama*.

4.1. Zaštita klijentskih računala

Zaštita na razini klijentskih računala najčešće se svodi na instalaciju specijaliziranih *antispam* alata kojima je namjena prepoznavanje i filtriranje *spam* poruka. Kvaliteta ovakvih alata ovisi o metodama filtriranja koje se koriste, i najčešće varira od proizvoda do proizvoda. Neke od najpopularnijih tehnika koje se koriste za prepoznavanje i filtriranje *spam* poruka uključuju korištenje regularnih izraza, *whitelist*, *blacklist* i DNSBL liste, Bayes filtriranje, Razor servis i sl.

4.1.1. Tehničke kontrole

Većina *antispam* alata namijenjenih instalaciji na klijentskim računalima funkcionira na principu *proxy* poslužitelja, koji se postavlja u komunikacijski kanal između korisničkog klijenta za pregledavanje elektroničke pošte i POP3, odnosno IMAP poslužitelja s kojeg se dohvaćaju e-mail poruke. Prilikom dohvaćanja novih poruka, one prolaze kroz *antispam* filtar, gdje se obavlja određena analiza zaglavlja i tijela poruke, na temelju čega se utvrđuje da li se radi o *spam* poruci ili ne. Poruke prepoznate kao *spam* najčešće se označavaju odgovarajućom oznakom u *Subject* polju, kako bi se na taj način korisniku olakšalo njihovo filtriranje nakon što se učitaju unutar klijenta elektroničke pošte. Primjer alata koji funkcioniraju na ovom principu su SpamPal i K9 alati koje je moguće dohvatiti s CARNet CERT-ovih Web stranica u kategoriji "Antispam alati" (http://www.cert.hr/tools.php?kw=&lang=hr&os=&cat=11). Osnovni nedostatak ovih alata je što, bez obzira radilo se o *spamu* ili ne, moraju dohvatiti sve poruke s e-mail poslužitelja.
Osim alata koji se baziraju na upravo spomenutoj *proxy* funkcionalnosti, također postoje i specijalni *antispam* alati namijenjeni kućnim korisnicima koji Internetu pristupaju korištenjem modema. Budući da je propusnost ovakvih linija vrlo mala, dohvaćanje svih poruka s e-mail poslužitelja može biti dugotrajan i mukotrpan proces. Za takve korisnike razvijeni su specijalni alati, koji ne dohvaćaju cijeli sadržaj poruke sa poslužitelja, već samo njeno zaglavlje. Na temelju pregledavanja zaglavlja, korisnik može prepoznati koje su poruke legitimne, a koje ne, te na temelju toga može dohvatiti samo one koje smatra potrebnima, a ostale može obrisati dok se još nalaze na poslužitelju. Ovakvim pristupom osim vremena, korisnici mogu uštedjeti i novac, budući da se znatno skraćuje vrijeme potrebno za dohvat e-mail poruka. Primjer alata koji funkcionira na ovom principu je EmC817 alat također dostupan na Web stranicama CARNet CERT-a.

4.1.2. Preventivne mjere

Osim programskih, odnosno tehničkih rješenja u vidu različitih *antispam* alata, korisnici se od *spama* mogu zaštiti i preventivnim mjerama koje će u prvom redu *spammerima* otežati dolazak do korisničkih adresa elektroničke pošte. Za razliku od tehničkih rješenja koja omogućuju detekciju i filtriranje *spam* poruka nakon što one već pristignu na adresu korisnika, preventivnim mjerama moguće je djelovati preventivno, odnosno moguće je smanjiti količinu neželjenih poruka.
Neke od preporuka kojima korisnici mogu zaštiti svoje adrese od dolaska na *spam* liste navedene su u nastavku:

- **Izbjegavati objavljivanja adresa elektroničke pošte na Web stranicama.** Roboti za automatsko prikupljanje adresa mogu u vrlo kratkom vremenu detektirati adresu te je automatski dodati na *spam* liste.
- **Izbjegavati objavljivanje adresa u izvornom obliku.** Ukoliko postoji potreba za objavljivanjem adresa elektroničke pošte na Web stranicama, preporučuje se korištenje alternativnih prikaza koji će zavarati automatizirane bot programe. Neki od primjera navedeni su u nastavku dokumenta.
- **Korištenje challenge/resposne *antispam* servisa.** Nakon što mail poslužitelj primi poruku od nepoznatog pošiljatelja, istome se vraća zahtjev za potvrdom kako bi se na taj način provjerila legitimnost poruke. Nakon primanja potvrde, koja zadovoljava određene kriterije, poslužitelj smatra da se radi o legitimnoj poruci te je isporučuje krajnjem korisniku. Ovaj koncept bazira se na činjenici da većina *spam* poruka lažira *From* polje poruke elektroničke pošte.
- **Korištenje različitih adresa za različite namjene.** Svim korisnicima preporučuje se korištenje različitih adresa elektroničke pošte za različite svrhe. Osim legitimne adrese koja se koristi za svakodnevno obavljanje korisničkih aktivnosti, preporučuje se registracija dodatnih adresa koje će se koristiti u drugim slučajevima (dohvaćanje besplatnog softvera, registracija na Web portalima i forumima i sl.). U tu svrhu najpraktičnije je iskoristiti besplatne servise kao što su Yahoo, Google i sl.
- **Disposable adrese elektroničke pošte.** Metoda koja se bazira na korištenju različitih aliasa e-mail adresa koje sve pokazuju na originalnu adresu korisnika. Prilikom ostavljanja e-mail adrese na nekom od servisa koji to zahtjeva, korisnici umjesto originalne adrese ostavljaju alias adresu koja se automatski povezuje sa stranicom gdje je ostavljena. Ukoliko na tu

adresu počinje pristizati *spam*, ona se automatski blokira (bez da se time utječe na originalnu korisničku adresu), a istovremeno je poznat i izvor s kojeg je poruka prikupljena. Više informacija o korištenju *disposal* adresa elektroničke pošte moguće je pronaći na sljedećim adresama:

- http://email.about.com/library/weekly/aa072002a.htm,
- http://email.about.com/cs/dispaddrrevs/,
- http://sneakemail.com/.

- **Ne koristiti jednostavna imena za adrese elektroničke pošte.** Prilikom otvaranja e-mail korisničkog računa paziti ime koje se odabire. Iako je poželjno da adresa bude jednostavna i laka za pamćenje, preporučuje se korištenje imena koja neće biti osjetljiva na *dictionary* napade malicioznih alata. Npr. umjesto adrese ime@example.com, preporučuje se korištenje adresa kao što su imeprezime@example.com ili imeBroj@example.com i sl.
- **Ne odgovarati na remove zahtjev.** Gotovo svaka *spam* poruka završava uputama kako se odjaviti s liste ukoliko korisnik više ne želi primati poruke. Na ove poruke ne preporučuje se nikada odgovarati, budući da se na taj način *spammerima* daje do znanja da je adresa aktivna i da korisnik koristi servis elektroničke pošte.
- **Koristiti usluge davatelja Internet usluga koji pružaju *antispam* zaštitu.** Za manje iskusne korisnike može se preporučiti korištenje servisa elektroničke pošte kod tvrtki koje nude *antispam* zaštitu. U tom slučaju odgovornost održavanja *antispam* alata stavljena je na davatelja usluge, a od korisnika se očekuje da razumije kako je koristiti za svoje potrebe.

4.1.3. Zaštita adresa elektroničke pošte na Web stranicama

Korisnici trebaju biti svjesni da su adrese objavljene na javnim Web stranicama pogodne za prikupljanje od strane automatiziranih programa za prikupljanje adresa (engl. *robots, bots*). Ovi programi adrese prikupljaju tako da pregledavaju sadržaj Web stranica i pritom traže sve one skupove znakova koji imaju oblik adrese elektroničke pošte (mailto:ime@domena). Kao test provjere vidljivosti e-mail adrese može poslužiti npr. poznata Web tražilica Google. Kao traženi pojam potrebno je unijeti korisničku adresu elektroničke pošte, a broj pronađenih stranica pokazati će na kojim je mjestima ona dostupna. Kako bi spriječili robote u prikupljanju adresu, poželjno je adrese prikazivati u alternativnim formatima, neprepoznatljivima za *bot* programe.

Neke od tehnika prikrivanja adresa navedene su u nastavku:

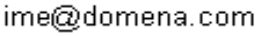
- **Modificiranje e-mail adresa.** Najjednostavnija metoda zaštite objavljenih adresa elektroničke pošte je modificiranje njenog prikaza tako da sadrži sve potrebne informacije, ali da je prikazana u izmijenjenom obliku. Npr. ubacivanje znakova razmaka ili drugih znakova može zbuniti programe za prikupljanje adresa, a da adresa još uvijek korisnicima bude razumljiva (npr. ime @ domena.com, imeMAKNI_ME@domena.com).
- **Korištenje ASCII ekvivalentnih znakova.** Ovom metodom znakove zamjenjujemo s njihovim ASCII ekvivalentima koje će korisnički Web preglednik pretvorit u odgovarajuće, korisniku razumljive znakove. Format prikaza je: `&#broj` koji odgovara određenom znaku;. Npr. adresa ime@domena.com biti će prikazana u formatu `ime&#64;domena&#46;com` (`&#64;` predstavlja znak „@“, a `&#46;` znak „.“). Više informacija o ASCII formatu moguće je naći na adresi http://www.ascii.cl/.
- **Korištenje skriptnih jezika.** Korištenjem skriptnih jezika kao što su JavaScript moguće je emulirati *mailto* funkciju koju HTML koristi za prikaz adresa elektroničke pošte. Ideja je da se na Web stranici kreira HTML veza (engl. *link*), koja korisničko ime i domenu adrese unosi u program koji će na temelju prenesenih vrijednosti kreirati upotrebljivu e-mail adresu. Više informacija o mogućnostima korištenja ove tehnologije te primjerima programa moguće je naći na adresi http://jamesthornton.com/software/redirect-mailto.html. Slijedeća Javascript funkcija omogućuje emuliranje prikaza e-mail adresa koji će onemogućiti detekciju od strane autiomatiziranih bot programa.

```
<a href='javascript:window.location = "mail" + "to:" + "user" + "@" +
"domain" + "." + " com";'
 onmouseover='window.status="mail" + "to:" + "user" + "@" + "domain" + "." +
"com";
 return true;'
 onmouseout='window.status="";
```

```
 return true;'
>Click here to send mail.</a>
```

Da bi ova skripta funkcionirala korisnički Web preglednik mora imati podršku za JavaScript jezik. Više informacija o opisanoj tehnici moguće je također naći na adresama http://www.macefficiency.com/me101/1999/46_PreventingSpam.html i http://automaticlabs.com/products/enkoderform/

- **Korištenje grafičkog prikaza umjesto tekstualnog.** Najučinkovitija zaštita adrese elektroničke pošte od *bot* programa je njen prikaz u obliku slike. E-mail adresu potrebno je prikazati grafički kao što je to prikazano na sljedećem primjeru:



Ovakav prikaz u potpunosti će onemogućiti sve *bot* programe.

4.2. Zaštita poslužiteljskih računala

Zaštita na razini poslužitelja specifična je po tome što se cijeli postupak filtriranja provodi na e-mail poslužitelju putem kojeg korisnici primaju elektroničku poštu. Odgovarajući *antispam* alat u ovom se slučaju integrira s e-mail poslužiteljem te se na taj način pregledavaju sve poruke namijenjene korisnicima računalne mreže na kojoj je poslužitelj postavljen. Ovisno o postavkama alata, poruke se mogu samo označiti kao *spam*, prebaciti u karantenu ili ih je moguće u potpunosti obrisati. Obzirom da pouzdanost niti jednog *antispam* alata nije 100%, u većini slučajeva preporučuje se označavanje poruka bez brisanja. Nakon što je poruka obilježena korisnik može upotrijebiti filtre unutar klijenta za pregledavanje elektroničke pošte kako bi ih izdvojio u zaseban direktorij.
Tehnike prepoznavanja i filtriranja *spam* poruka slične su kao i kod klijentskih programa, iako je podešavanje i način rada alata nešto drugačiji. S obzirom da se alat integrira s e-mail poslužiteljem, podešavanje alata ovisit će o mail poslužitelju i operacijskom sustavu koji se koristi. Na Linux sustavima najpoznatiji alat za filtriranje *spam* poruka je SpamAssassin koji je ujedno i besplatan, dok su za Windows sustave dostupni brojni komercijalni programi različitih proizvođača.
Jedan od nedostatka filtriranja *spam* poruka na strani poslužitelja je taj što korisnici u većini slučaja nisu u mogućnosti prilagođavati parametre filtriranja svojim potrebama. S obzirom na specifičnost poruka koje korisnici primaju, ovaj problem može u određenim situacijama predstavljati problem. Iako neki od alata podržavaju mogućnost definiranja pravila filtriranja za pojedine korisnike, u praksi se ova funkcionalnosti rijetko koristi.
Prednosti zaštite na razini e-mail poslužitelja u odnosu na zaštitu na razini klijenta su:

- instalacijom na poslužitelju eliminirani su problemi kompatibilnosti koji se mogu javiti kod instalacije na klijentskim računalima,
- smanjuju se troškovi licenciranja alata,
- osigurava se centralno filtriranje poruka što smanjuje administrativni angažman,
- koriste se naprednije funkcionalnosti.

U nastavku su navedene neke od tehnika koje administratori e-mail poslužitelja mogu primijeniti u svrhu podizanja razine sigurnosti i zaštite svojih korisnika od *spam* poruka.

4.2.1. Zabrana neautoriziranog slanja poruka elektroničke pošte

Open relay poslužitelji danas su vrlo opasni, budući da ih *spammeri* redovito koriste za masovno prosljeđivanje poruka elektroničke pošte, a da pritom u određenoj mjeri ostanu anonimni. Također, legitimni e-mail poslužitelji koji se ponašaju kao *open relay* i koje *spammeri* koriste za slanje *spam* poruka vrlo će se brzo naći na "crnim listama", što će onemogućiti daljnje slanje poruka budući da velik broj e-mail poslužitelja ne prihvaća konekcije s tih adresa. Na URL adresi http://rbls.org/ moguće je naći veze na velik broj crnih lista koje se mogu koristiti u okviru *antispam* zaštite. Blokiranjem konekcija s adresa tih e-mail poslužtelja znatno se može smanjiti količina *spam* poruka, budući da je poznato da se radi o nepouzdanim adresama koje su poznate kao izvor *spam* poruka. Nedostatak korištenja crnih lista je taj što ukoliko neki od legitimnih e-mail poslužitelja pogreškom dospije na neku od njih, sve poruke koje dolaze s te adrese biti će također odbijene.
Na sljedećim adresama također je moguće naći detaljne informacije o tome kako onemogućiti neautorizirano slanje poruka elektroničke pošte na nekim od popularnijih e-mail poslužitelja:

- SendMail, http://www.sendmail.org/tips/relaying.html,

- MS Exchange, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/mailexch/excrelay.asp
- Exchange 2000, http://support.microsoft.com/view/tn.asp?kb=319356

4.2.2. Filtriranje poruka elektroničke pošte

U sklopu rada e-mail poslužitelja preporučuje se instalacija odgovarajućeg *antispa*m alata koji će centralno filtrirati i označavati *spam* poruke. Detekcijom i označavanjem *spam* poruka na e-mail poslužitelju korisnicima se olakšava njihovo prepoznavane i dodatno filtriranje unutar svojih klijenta elektroničke pošte. Pritom treba voditi računa da se broj lažno detektiranih poruka svede na najmanju moguću mjeru, budući da korisnici vrlo često automatski brišu sve poruke označene kao *spam*. Kako bi se podigla razina pouzdanosti filtriranja poruka, preporučuje se kombiniranje različitih tehnika kao što su Bayes, Razor, DCC, *blackliste* i sl.

- **Bayes filtar.** Jedna od tehnika koja je iznimno pridonijela pouzdanosti prepoznavanja *spam* poruka. Poruka elektroničke pošte se parsira i iz nje se izvlače svi nizovi znakova kao što su riječi, brojevi, Internet adrese, itd. Svakom nizu dodjeljuje se vjerojatnost u postocima, zasnovana na učestalosti njegovog pojavljivanja u prijašnjim porukama. Vrijednost se računa prema izrazu:

$$\frac{\frac{SH}{TS}}{\frac{SH}{TS}+\frac{IH}{TI}}$$

Značenje pojedinih parametara je sljedeće:

- SH (engl. *spam hits*): *spam* pogodci.
- TS (engl. *total spam messeges*): ukupan broj *spam* poruka.
- IH (engl. *innocent hits*): nedužni pogodci.
- TI (engl. *total innocent messeges*): ukupan broj nedužnih poruka (ne-*spam* poruka).

Rezultat je u granicama od 0 do 1, pri čemu vrijednost 1 opisuje niz koji sigurno karakterizira dio *spam* poruke, a vrijednost 0 niz koji karakterizira dio legitimne poruke. Ukoliko se niz nikada nije pojavio u prijašnjim porukama, ili nije prešao minimalni prag, dodjeljuje mu se neutralna vrijednost koja ga uklanja iz daljnjih provjera. Dodijeljene vjerojatnosti koriste se za određivanje statističke vjerojatnosti koja opisuje da li je neka poruka *spam* ili ne. Ovakav pristup omogućuje detekciju *spam* poruka sa 90-99 % sigurnošću, te sa samo 0.01 % - 3 % lažnih detekcija. Npr.

Vjerojatnost	Niz
0.9901	Url*unsub
0.9901	div+align
0.9901	font+color
0.9901	Unsub
0.0100	Support
0.0100	Stuff
0.0100	have+the
0.0101	this+stuff
0.9865	Receiving
0.9830	Click
0.9663	Subject*hot
0.9586	Special
0.0458	Love
0.9539	Offers
0.9521	Below

Tablica 1: Vjerojatnosti nizova poruka elektroničke pošte

15 nizova znakova prikazanih u gornjoj tablici identificirani su kao najinteresantniji nizovi iz poruke elektroničke pošte, gdje se njihova interesantnost određuje pomoću udaljenosti njegovih vjerojatnosti od 0.5, odnosno 50 %.

Primjenom Bayesianovog statističkog teorema koji glasi:

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

gdje parametri P(A) i P(B) predstavljaju vjerojatnosti događaja A i B, zbrajaju se sve vjerojatnosti i dobiva se vrijednost između 0 i 1. Što je rezultat bliži 1 veća je vjerojatnost da je poruka *spam*. Cijeli projekt filtriranja *spam* poruka temeljen na Bayes algoritmu inspiriran je dokumentom Paul Grahama koji se dostupan na adresi http://www.paulgraham.com/spam.html.

- **DCC (*engl. Distributed Checksum Clearinghouse*).** DCC je servis koji je zasnovan na pretpostavci da se *spam* poruke šalju na velik broj e-mail adresa. Sustav se sastoji od tisuća klijentskih i par stotina poslužiteljskih računala koja na dnevnoj bazi obrađuju milijune poruka elektroničke pošte te na temelju njih generiraju odgovarajuće potpise koji se kasnije koriste za detekciju *spam* poruka. *Mail transfer* i *user* agenti spajaju se na javne DCC poslužitelje koji primljene poruke uspoređuju s *checksum* potpisima identificiranih, ranije prepoznatih *spam* poruka na temelju čega klijentu vraćaju odgovor o obavljenoj provjeri. DCC servis bazira se na ideji da se klijentima omogući detekcija *spam* poruka na temelju usporedbe sa porukama koje primaju drugi korisnici sustava elektroničke pošte. Više informacija o korištenju DCC servisa i njegovim mogućnostima moguće je pronaći na URL adresi http://www.rhyolite.com/anti-spam/dcc/.
- **Razor.** Vipul's Razor je distribuirani javni servis namijenjen detekciji i filtriranju *spam* poruka. Razor servis bazira se na aktivnom sudjelovanju većeg broja Internet korisnika, na temelju čega se kreira distribuirani, redovito osvježavani katalog *spam* poruka koji klijenti mogu koristiti za filtriranje neželjenih poruka elektroničke pošte. Detekcija nelegitimnih poruka provodi se kombinacijom statističkih metoda i potpisa kreiranih na temelju detektiranih *spam* poruka, čime se omogućuje efikasno prepoznavanje poznatih, ali i novo osmišljenih formata *spam* poruka. Više informacija o Razor servisu moguće je pronaći na adresi http://razor.sourceforge.net/.
- **Blacklist i whitelist liste**. *Blackliste* su baze IP adresa poznatih *spammera* i e-mail poslužitelja koji su izvor *spam* poruka. E-mail poslužitelj koji se nalazi na jednoj od takvih lista neće biti u mogućnosti slati poruke elektroničke pošte, ukoliko primatelj blokira primanje poruka s IP adresa navedenih u *blacklistama*. Nakon dodavanja poslužitelja na "crnu listu", nadležnima za tu IP adresu biti će poslana odgovarajuća obavijest, zajedno s uputama što učiniti kako bi se on uklonio sa *blackliste*. Moguće je da se na takvoj *blacklisti* nađe i IP adresa legitimnog mail poslužitelja što može predstavljati ozbiljan problem za administratore, budući da je uklanjanje poslužitelja s *blackliste* puno teže nego dolazak na nju. Za razliku od *blacklista*, *whiteliste* su baze pouzdanih IP adresa sa kojih prihvaćamo poruke elektroničke pošte.

4.2.3. Prijava *spam* i *nospam* poruka

Administratorima e-mail poslužitelja preporučuje se definiranje posebnih adresa na koje korisnici mogu prijaviti spam poruke koje su zaobišle antispam filtar, kao i poruke koje su pogrešno prijavljene kao spam. Poruke koje korisnici pošalju na ove adrese mogu se iskoristiti za treniranje Bayes filtra kako bi se slične poruke u budućnosti ispravno označile.

Prilikom odabira adresa na koje korisnici mogu prijaviti pogrešno označene poruke, treba voditi računa o njihovom imenu budući da i one mogu postati mete spammera. Ukoliko se poštanski sandučići ovih adresa koriste za automatsko treniranje Bayes filtara, moguće je postići negativan utjecaj.

4.2.4. Zaštita sekundarnih e-mail poslužitelja

Budući da gotovo sve organizacije za primanje elektroničke pošte koriste nekoliko MX poslužitelje, koji su u javnom DNS poslužitelji navedeni kao MX zapisi različitih prioriteta, *antispam* zaštitu potrebno je implementirati na svakom od njih. Ukoliko to nije slučaj, *spammeri* za slanje elektroničke pošte mogu iskoristiti sekundarne poslužitelje te na taj način zaobići *antispam* zaštitu.

Ukoliko sekundarni MX poslužitelji nisu pod kontrolom organizacije, potrebno je vidjeti da li organizacija uopće treba sekundarne poslužitelje s obzirom da se time povećavaju troškovi *antispam*

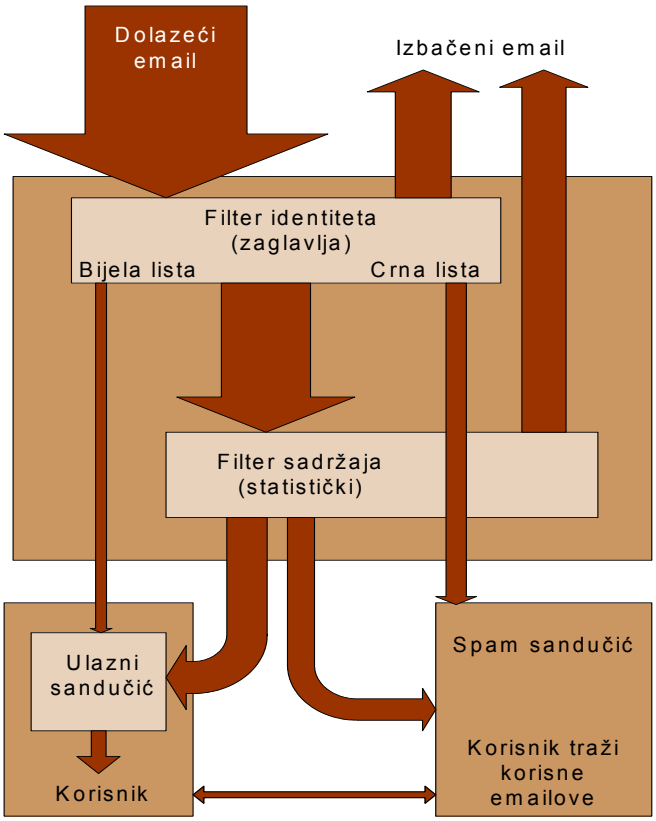
zaštite. Sekundarni poslužitelji poželjni su kod organizacija koje primaju velike količine elektroničke pošte, gdje takvi poslužitelji obavljaju funkciju raspodjele opterećenja (engl. *load balancing*). Ukidanje takvih poslužitelja rezultiralo bi preopterećenjem primarnog poslužitelja, što je svakako neprihvatljivo.
Ukoliko sekundarni e-mail poslužitelji obavljaju funkciju redundantnosti, odnosno preuzimaju funkciju primanja elektroničke pošte u slučaju pada primarnog MX poslužitelja, možda ih je u potpunosti moguće ukloniti. Ukoliko je primarni e-mail poslužitelj neko vrijeme nedostupan to ne mora predstavljati kritični problem pošto će neispostavljene poruke čekati u redu poslužitelja koji šalje poruku. Nakon ponovne uspostave primarnog MX poslužitelja poruke će biti uredno isporučene.

4.2.5. Blokiranje pristupa ostalim e-mail poslužiteljima

Prema svim e-mail poslužiteljima koji nisu navedeni kao MX zapisi u DNS bazi javnog poslužitelja potrebno je onemogućiti pristup prema TCP portu 25 putem kojeg se odvija SMTP komunikacija. Sav dolazni e-mail promet mora proći kroz javne e-mail poslužitelje organizacije, koje je samim time potrebno kao MX zapise unijeti u bazu javnog DNS poslužitelja.
Ovo pravilo osim za e-mail poslužitelje, vrijedi i za sve ostale servise koji su lokalnog značaja i koji ne trebaju biti dostupni s javnog Interneta.

5. Arhitektura *antispam* alata

U borbi protiv *spama* najznačajniju ulogu igraju svakako specijalizirani *antispam* alati. Danas na tržištu postoji velik broj komercijalnih i *antispam* alata, čija je pouzdanost prilično visoka. Većina ovih alata *spam* poruke će detektirati s vjerojatnošću iznad 90%, što je više nego zadovoljavajuće obzirom na probleme koje *spam* stvara korisnicima informacijskih sustava. Za filtriranje *spam* poruka alati redovito kombiniraju nekoliko različitih metoda kako bi se na taj način podigla razina pouzdanosti i smanjio broj lažnih upozorenja.
Na slici 2 prikazana je arhitektura jednog tipičnog *antispam* alata koji se instalira u kombinaciji sa e-mail poslužiteljem. Prikazani alat kombinira tehnike Bayesianovog (statističkog) filtriranja i filtriranja pomoću *blacklista* i *whitelista*.



Slika 2. Filtriranje e-mail poruka

Svaka poruka elektroničke pošte koju e-mail poslužitelj prihvati šalje se na analizu *antispam* alatu koji je postavljen na poslužitelju.-Način na koji se poruka prosljeđuje ovisi o vrsti alata i operacijskom sustavu na kojem se koristi. Na Linux operacijskom sustavu u tu se svrhu najčešće koristi amavisd poslužitelj koji se ponaša kao sučelje između e-mail poslužitelja i ostalih programa za analizu sadržaja poruka elektroničke pošte. Primjer uspostave sustava *antispam* i antivirusne zaštite na Linux operacijskim sustavima korištenjem Clamav i SpamAssassin alata opisan je u CARNet CERT dokumentu pod nazivom "Implementacija antivirusne i *antispam* zaštite na Linux OS-u korištenjem ClamAV i SpamAssassin programskih paketa" na adresi http://www.cert.hr/filehandler.php?did=107.

6. Napredne metode filtriranja *spam* poruka

Obzirom na probleme koje *spam* predstavlja za korisnike Interneta, u borbu protiv *spam*-a uključile su se brojne velike tvrtke i organizacije kao što su Microsoft, AOL, Yahoo, Earthlink i drugi. Osim brojnih tehnoloških rješenja koja bi trebala pomoći u suzbijanju *spam*-a, velik korak napravljen je i na području zakonske regulative kojom se regulira slanje neželjene elektroničke pošte.
Nove tehnologije i rješenja kojima se problem *spam*-a na stoji suzbiti na prihvatljivu razinu svakodnevno se pojavljuju, a u nastavku su navedene neke od njih.

- **Caller ID.** Tehnologija osmišljena od strane Microsofta, koja se bazira na ideji da organizacije u svoje DNS poslužitelje, osim dolaznih MX poslužitelja zaduženih za primanje poruka elektroničke pošte, navedu i one odlazne, koji se koriste za slanje poruka elektroničke pošte. Primatelj poruke bi na temelju *From:* polja dolazne poruke mogao provjeriti da li je ista poslana s legitimnog e-mail poslužitelja koji je registriran kao odlazni MX poslužitelj domene čije je ime navedeno u poruci. Na ovaj način bi za svaku poruku bilo moguće provjeriti da li zaista dolazi sa domene koja je navedena u samoj poruci. Više informacija o osnovnim konceptima i mogućnostima primjene Caller ID tehnologije moguće je naći na adresi http://www.microsoft.com/mscorp/twc/privacy/spam_callerID.mspx.

- **DomainKeys.** Tehnologija ponuđena od strane Yahoo-a koja se trenutno testira u suradnji sa Sendmail konzorcijem. Iako se metoda također bazira na identifikaciji pošiljatelja elektroničke pošte, princip rada znatno se razlikuje u odnosu na Caller ID tehnologiju. Korištenjem asimetrične *public/private key* kriptografije, u zaglavlje svake poruke odlazni mail poslužitelj dodaje digitalni potpis potpisan privatnim ključem organizacije. Javni ključ kojim je moguće provjeriti autentičnost poruke, organizacija objavljuje su u javnom DNS poslužitelju, kako bi se na taj način stavio na raspolaganje svim ostalim korisnicima Intereta. Pri primanju poruke dolazni e-mail poslužitelj provjerava digitalni potpis korištenjem javnog ključa organizacije. Ukoliko je potpis valjan, poruka se prosljeđuje korisniku na kojeg je adresirana, dok se u suprotnom smatra lažiranom. Više informacija o DomainKeys tehnologiji moguće je naći na adresi http://docs.yahoo.com/docs/pr/release1143.html.
- **Sender Policy Framework (SPF).** SPF je tehnologija osmišljena od strane AOL organizacije i trenutno je također u fazi testiranja. Slično kao i Caller ID, SPF tehnologija zahtjeva autentikaciju pošiljatelja. Ukoliko se IP adresa pošiljatelja ne podudara s IP adresom domene s koje je navodno došao e-mail, e-mail će biti odbačen i prije nego stigne do korisničkog poštanskog sandučića. Tu tehnologiju zagovara grupa SMTP+SPF. Više informacija o ovoj tehnologiji može se dobiti na adresi http://spf.pobox.com/.
- **Sender ID.** Radi se o tehnologiji koju zastupa Microsoft, a koja bi napokon trebala stati na kraj *spamu* ili barem smanjiti njegovu količinu na prihvatljivu razinu. Sender ID je način osiguravanja potvrde da e-mail poruka dolazi s adrese koja je u zaglavlju navedena kao izvorišna adresa, a tehnologija se oslanja na ranije predložena rješenja Caller ID i Sender Policy Framework (SPF). Za sada je već nekolicina tvrtki najavila podršku za Sender ID u svojim aplikacijama i to: Cloudmark, DoubleClick, IronPort Systems, Sendmail, Symantec, Tumbleweed i VeriSign.
- **SSL/TLS (Secure Sockets Layer/ Transport Layer Security) enkripcija.** Za zaštitu poruka elektroničke pošte također je moguće koristiti i protokole kao što su Secure Socket Layer (SSL) i Transport Layer Security (TLS). Budući da protokoli kao što su SMTP, POP i IMAP inicijalno poruke mrežom šalju u čistom tekstualnom obliku, korištenjem navedenih algoritama moguće je osigurati njihovu povjerljivost. Iako korištenje navedenih algoritama neće izravno pomoći u suzbijanju *spam*-a, njihova upotreba može znatno podići razinu sigurnosti sustava elektroničke pošte.
- **Greylisting.** *Greylisting* tehnologija naziv je dobila po tome što kombinira obilježja *blacklist* i *whitelist* lista. Ova metoda je vrlo jednostavna i bazira se na tri osnovne informacije koje čine poruku elektroničke pošte:
  1. IP adresa računala koje pokušava dostaviti poruku,
  2. adresa pošiljatelja i
  3. adresa primatelja.

  Ove informacije dovoljne su da se s određenom razinom pouzdanosti može utvrditi da li se radi o legitimnoj ili *spam* poruci. Ukoliko primljena poruka sadrži kombinaciju navedenih elemenata koji su prvi puta viđeni, poruka se može odbiti. *Greylisting* tehnologija trebala bi smanjiti broj lažnih upozorenja u postupku detekcije *spam* poruka. Više informacija o *greylisting* tehnologiji moguće je naći na adresi http://projects.puremagic.com/greylisting/ .

7. Zakonska regulativa

Zakonske regulative i pravilnici svakako su jedan od najznačajnijih koraka u suzbijanju *spam* poruka. Mnoge države već su donijele zakone vezane uz neželjenu elektroničku poštu, a već su poznati i brojni primjeri njihovog provođenja. Što su zemlje tehnološki naprednije to je veća vjerojatnost da imaju zakone kojima se kontrolira slanje neželjene elektroničke pošte. SAD kao zemlja koja je trenutno najveći izvor *spam*-a najviše je napredovala u ovom području. Jedan od problema zakonske regulative je taj što za potpunu učinkovitost sustava sve zemlje moraju prihvatiti takav zakon, budući da u suprotnom *spammeri* svoje aktivnosti mogu provoditi u ostalim zemljama koje to područje nemaju pravno regulirano.

7.1. SAD

Američki predsjednik George W. Bush potpisao je zakon koji bi trebao spriječiti da Amerikanci primaju i šalju neželjene poruke elektroničke pošte. Zakon je prihvatio američki Kongres krajem 2003. godine, a njime se stavlja izvan zakona slanje neželjenih poruka koje komercijalni oglašivači svakodnevno upućuju na stotine milijuna adresa elektroničke pošte kako bi prodali svoje proizvode ili usluge. Prema novom zakonu, potrošači mogu izabrati da ne primaju neželjene poruke, a pošiljatelji koji ne budu poštovali njihovu odluku mogu se suočiti s visokim novčanim kaznama ili čak kaznama od nekoliko godina zatvora.

7.2. Europska Unija

U EU je slanje poruka elektroničke pošte komercijalnog sadržaja kazneno djelo, ukoliko primatelj nije zatražio da ih prima. Tvrtke i pojedinci koji nastave slati *spam* poruke suočit će se s visokim novčanim kaznama. U određenih slučajevima, po novim EU zakonima, primatelj će moći tužiti tvrtke.

7.3. Hrvatska

U Hrvatskoj također postoji zakon o *spamu*. Problematiku *spama* uređuje Zakon o telekomunikacijama. Člankom 111. definirano je što se smatra *spamom* (neželjenim telekomunikacijskim priopćenjima), uvjete pod kojima se i na koji način takva priopćenja mogu slati, te za prekršitelje predvidio visoke novčane kazne (članak 116. st. 40). Za više detalja o Zakonu o telekomunikacijama pogledati na stranici http://www.nn.hr/clanci/sluzbeno/2003/1731.htm .

7.4. Ostale zemlje

Ostale zemlje, one manje napredne (tehnološki inferiornije od SAD-a i EU-a), imaju svoje zakone protiv *spama*. Od ostalih zemalja sa zakonom treba spomenuti Argentinu, Australiju, Brazil, Kanadu, Češku, Indiju, Japan, Rusiju, Južnu Koreju i Srbiju i Crna goru.

8. Zaključak

Iako je *spam* već dugi niz godina jedan od najozbiljnijih problema Interneta, količina *spam* poruka koje svakodnevno pune poštanske sandučiće korisnika se ne smanjuje. Bez obzira na brojne tehnologije, programske pakete i zakonsku regulativu, *spam* i dalje predstavlja vrlo velik problem za gotovo sve korisnike Interneta. Osim pojašnjenja osnovnih pojmova i tehnologija vezanih uz *spam*, dokument daje i pregled niza metoda koje korisnici i sistem administratori mogu iskoristiti za zaštitu od *spam*a. Opisane su metode i alate za zaštitu klijentskih i poslužiteljskih računala, preporuke za objavljivane adresa elektroničke pošte na javnim Web stranicama, postupci kako analizirati zaglavlja poruke i identificirati njenog pošiljatelja te brojni drugi aspekti vezani uz neželjenu elektroničku poštu.

9. Reference

[1] http://www.faqs.org/rfcs/rfc2505.html -RFC 2505 - Anti-Spam Recommendations for SMTP MTAs
[2] http://www.paulgraham.com/antispam.html - Paul Graham, Spam
[3] http://www.secinf.net/antispam/DealingEffectivelywithSpam.html - Dealing Effectively with Spam
[4] http://www.sendmail.org/antispam.html - Anti-Spam Provisions in Sendmail 8.8
[5] http://www.securityfocus.com/infocus/1763 - Anti-Spam Solutions and Security