*XXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2008**, Beograd, 16. i 17. decembar 2008.*

UNAPREĐENJE IMPLEMENTACIJE MODELA ANTI-SPAM ZAŠTITE

Snežana Mladenović, Slobodan Mitrović, Slađana Janković
Univerzitet u Beogradu – Saobraćajni fakultet

Sadržaj: *Anti-spam zaštita je postala sastavni deo softverskih paketa koji su namenjeni podizanju bezbednosti na nivou servera i klijenata. Rad predstavlja rešenje za poboljšanje efikasnosti anti-spam zaštite na e-mail serveru baziranom na Postfix-u.*

Ključne reči: *Anti-spam zaštita, SpamAssassin, Postfix, SMTP, Mailgraph, Monitoring*

1. Uvod

Anti-spam zaštita *e-mail* servera postala je, u poslednjih nekoliko godina, najvažniji deo zaštite korisnika *e-mail* servisa. Do pre nekoliko godina provajderi internet usluga su određivali antivirusnu zaštitu *e-mail* servera kao prioritetni vid poboljšanja svoje usluge sa stanovišta bezbednosti. Danas je situacija drastično izmenjena i na prvo mesto na listi prioriteta je postavljena zaštita od spama. Razlog za to je veoma uočljiv – udeo spama u ukupnoj količini poruka se drastično uvećava. Rezultati analiza u drugom kvartalu 2008. godine pokazuju veoma zabrinjavajuće podatke – udeo spam poruka, koji je u prva tri meseca 2008. godine iznosio 92.3% je do juna iste godine skočio na 96.5% [1]. Zapravo, korporacije se susreću sa činjenicom da od 28 primljenih *e-mail* poruka samo jedna ima koristan sadržaj. Sa sličnim problemima u približnim razmerama se susreću i ostali, nekomercijalni, korisnici internet usluga. Provajderi internet usluga, zavisno od svojih finansijskih potencijala i razvojnih resursa, mogu se zaštititi kupovinom komercijalnog softvera od proizvođača antivirusnih i anti-spam rešenja, ili upotrebom kombinovanih GPL (*General Public Licence*) antivirusnih i anti-spam rešenja sa sopstvenim razvojnim potencijalima ili unajmljenim uslugama. Upravo su GPL rešenja sa otvorenim kodom posebno interesantna sa stanovišta optimalnog odnosa ulaganja u zaštitu i dobijenog nivoa bezbednosti.

2. Klasifikacija spam mehanizama

U raznim publikacijama se može pronaći više različitih definicija za spam [2,3,4,5]. Uopšteno, ovaj pojam se može opisati kao poruka, čiji se sadržaj nameće primaocu bez njegove volje i koja stiže na adresu primaoca bez njegove saglasnosti i gde ne postoji nikakva direktna ili indirektna veza između pošiljaoca i primaoca. Spam se

može grubo podeliti u nekoliko kategorija u zavisnosti od njegovog sadržaja i mehanizma širenja:

- **prema sadržaju:**
  - masovne poruke neželjnog sadržaja (*Unsolicited bulk e-mail* - UBE),
  - masovne poruke komercijalnog sadržaja (*Unsolicited commercial e-mail* - UCE, *spamvertizing*),
  - masovne poruke sa sadržajem koji ima intenciju prevare primaoca (*fraudulent, 419 scams, phishing, mainslease,* itd.);

- **prema mehanizmu širenja:**
  - upotrebom robota i lažiranjem podataka izvorišne adrese (*botnets – zombie networks*),
  - eksploatacijom zaraženih računara,
  - upotrebom *open-relay mail* servera,
  - upotrebom *open-proxy* servera,
  - upotrebom javnih *(web)mail* servisa,
  - upotrebom mobilnih telefona.

Postoji širok spektar načina za širenje spam poruka zahvaljujući, pre svega, zastarelosti SMTP protokola koji u sebi ne sadrži bezbednosne mehanizme.

3. Metode blokade spam poruka

Veliki broj softverskih paketa za anti-spam zaštitu koristi kombinaciju dve ili više metoda za detekciju [6] i eliminaciju neželjenih poruka:

- "**Blekliste**" (crne liste, *Blacklists*) su DNS liste na kojima se nalaze izvori spama (*DNS-based blacklists, DNSBL*) ili liste izvorišnih *e-mail* adresa. Filter poredi izvorišnu adresu ili domen sa sadržajem baza podataka koje se preuzimaju sa specijalizovanih servisa ili su formirane na nivou korisnika. Navedeni mehanizam nije u potpunosti efikasan zbog činjenice da liste, po pravilu, ne sadrže kompletan spisak spamera. Takođe, odluke koje su bazirane na upotrebi navedenih listi mogu biti i pogrešne, zbog prisustva domena ili *e-mail* adresa koje su greškom identifikovane kao izvori spama.
- **HASH filter** je mehanizam zaštite baziran na formiranju jedinstvenog potpisa (*hash*) svake poruke u sistemu. Navedeni potpis se poredi sa uzorcima spam potpisa i, na osnovu navednog poređenja, donosi se odluka da li je poruka korisna ili ne. Ovaj metod ne daje značajne rezultate zbog činjenice da spameri često prave male izmene u svojim spam porukama, što dovodi do pojave različitih potpisa za poruku koja ima, smisaono posmatrano, istovetno značenje za primaoca.
- **Filter baziran na klasifikaciji teksta poruke** uključuje klasifikaciju po ključnoj reči, frazi ili po setu karaktera koji sadrži tekst poruke, na osnovu koje se dalje vrši proračun verovatnoće da li je pismo spam ili ne.

- **Filter baziran na setu pravila** (*Rule-based filtering*) funkcioniše tako što se uzorci spam poruka (delovi naslova poruke, datum slanja poruke, delovi *header*-a, itd.) formatirani kao ključne reči ili heuristički set pravila, porede sa odgovarajućim delom poruke za koju se formira odluka da li je spam ili ne. Setovi pravila mogu biti formirani i od strane korisnika. Nedostatak ove tehnike je potencijalno veliki procenat korisnih pisama, pogrešno prepoznatih kao spam (*false positives*).
- **Multiagent sistem filtriranja** je zasnovan na razmeni naučenih informacija o spam porukama između klijenata. Arhitektura ovog sistema inkorporira i prethodno navedene metode čime se poboljšava podrška odlučivanju.

4. SpamAssassin

SpamAssassin [7] je softver za detekciju spama. Pripada GPL grupi softvera sa otvorenim kodom. Koristi širok spektar testova za detekciju spama. Njegove najvažnije osobine su modularna struktura, koja mu daje mogućnost integracije sa većinom serverskih rešenja za distribuciju elektronske pošte, kao i skalabilnost, odnosno mogućnost proširenja njegove funkcionalnosti i povećanje efikasnosti lakom implementacijom novih mehanizama detekcije. Takođe, moguća je integracija i na nivou klijenta.

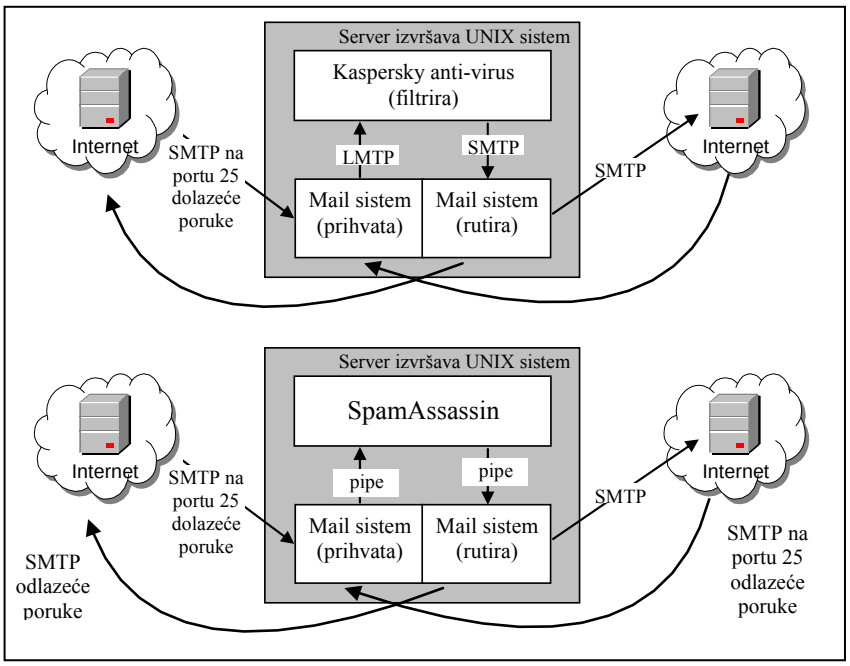
Osnovne metode detekcije koje koristi navedeni softver su:

- test *header*-a u porukama,
- testovi fraza u samom tekstu poruke,
- statistička Bayes-ovska analiza,
- automatski i manuelni *Whitelisting/Blacklisting,*
- kolaborativna identifikacija spama (upotrebom DCC-a, Pyzor-a, Razor2-a)
- upotreba "bleklista",
- detekcija bazirana na karakter setu.

Anti-spam i antivirusna zaštita se na nivou servera i klijenta realizuju u vidu filtera na transportnom sloju OSI modela. Implementacija se može vrlo jednostavno objasniti ukoliko se iskoristi primer servera. Pretpostavimo da MTA (*Mail Transfer Agent*) na serveru koristi SMTP protokol za komunikaciju. Komunikacija ka serveru se obavlja preko TCP porta 25. MTA, zatim, vrši procesiranje poruke upotrebom lokalne *loop* adrese 127.0.0.1 i više različitih portova, što zavisi od tipa MTA i njegovog toka lokalne obrade poruke. U osnovi, integracija se vrši presecanjem komunikacije procesa obrade poruke na pogodnom mestu i uvođenjem još jednog kanala obrade (filtera) na definisanom setu portova (ulazni i izlazni). Ukoliko su rešenja za antivirusnu i anti-spam zaštitu različita, onda se navedeni postupak izvodi posebno za svako rešenje.

U slučaju integracije SpamAssassin-a sa MTA tipa Postfix, integracija se vrši upotrebom opcije slične *content* filteru preko aktivacije *smtp* agenta, slika 1. Nakon ulaska u sistem, poruke bivaju prosleđenje u *queue* menadžer, nakon čega se za dodatne opcije može aktivirati *pipe* proces, zahvaljujući kome se može izvršiti implementacija posebno napisanog skripta, koji u svom sadržaju opisuje način ulaska poruke u filter,

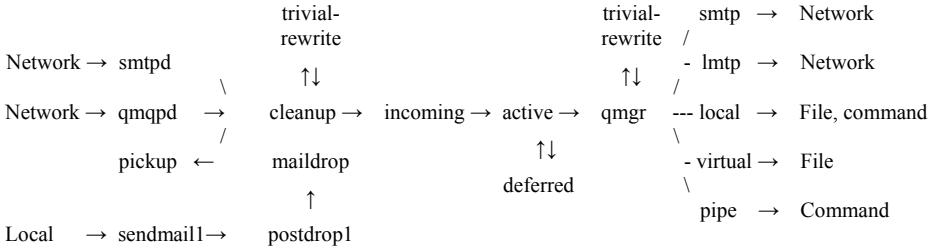
način postupanja sa porukom u slučaju da je SpamAssasin utvrdio da je poruka, zapravo, spam, i načine izlaska iz filtera. Lokacija samog skripta može biti definisana u mapi lokalnog SMTP transporta.



Slika 1. *Integracija antiuvirusnog i ant-ispam filtera na e-mail serveru baziranom na Postfix-u*

5. Zaštita na nivou MTA – primer Postfix-a

Postfix [8] je program koji ima ulogu MTA, odnosno ima zadatak da vrši rutiranje i isporuku elektronske pošte. Njegove osnovne osobine su brzina i lako administriranje. Postfix funkcioniše preko više različitih modula, inkorporiranih u njegovu arhitekturu, kao i upotrebom spoljnih entiteta, kao što su *smtpd* ili *qmqpd* server. Slika 2. pokazuje arhitekturu prijema i obrade poruke. Navedeni serveri skidaju *stmp* ili *qmqp* enkapsulaciju i šalju Postfix-u koristan sadržaj. Pre ulaska navedenog sadržaja u *cleanup* serverski modul, moguće je iskoristiti *smtpd* server za filtraciju jednog dela spam poruka.



Slika 2. *Arhitektura Postfix Mail Transfer Agenta (MTA)*

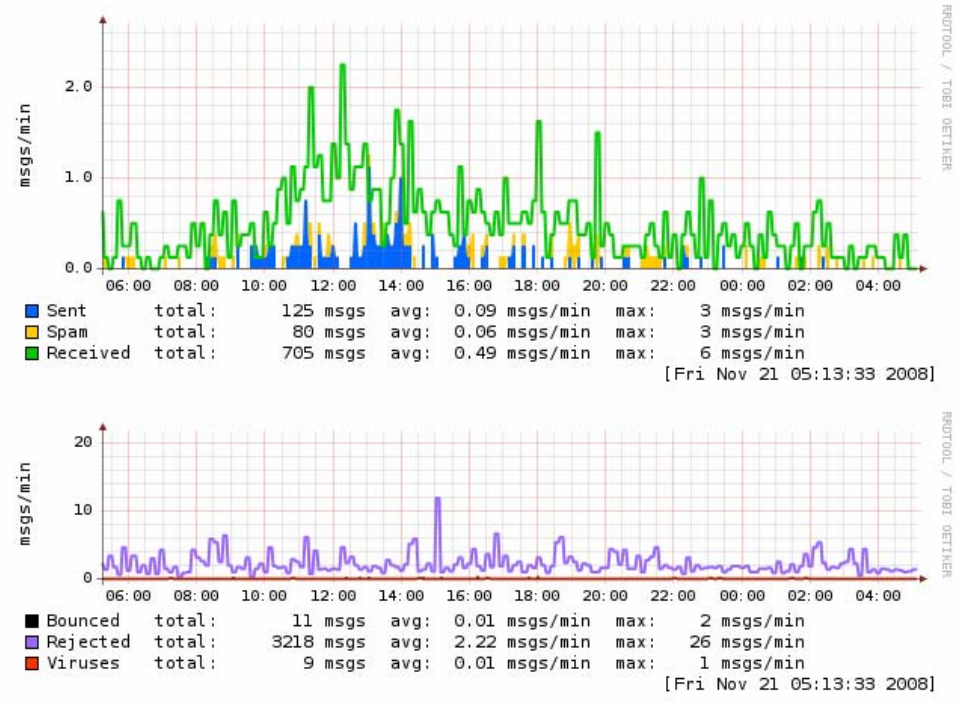
Filtracija (set restrikcija) se može izvesti na nivou podatka o klijentu, pošiljaocu ili primaocu poruke i to prema tačno utvrđenom redosledu. "Najčistija" filtracija se vrši na nivou primaoca prema sledećem redosledu [9]:

1. Zabraniti HELO/EHLO verifikaciju adrese primaoca.
2. Blokirati spoljni neautorizovani *pipelining* (osim u slučaju Postfix-a 2.x – ovu opciju treba primeniti na *smtpd_data* nivou zbog bolje iskorišćenosti resursa).
3. Dozvoliti protok poruka koje potiču sa lokalne mreže.
4. Odbaciti sve poruke koje u svojoj destinaciji nemaju adrese lokalne mreže.
5. Verifikovati ispravnost destinacione adrese (proveriti da li adresa primaoca zaista postoji na listi lokalnih korisnika).
6. Proveriti lokalne crne i bele liste na nivou pošiljaoca i primaoca.
7. Proveriti adresu pošiljaoca, domen i adresu pošiljaoca proverom DNSbl i RHSbl listi.

Najveći broj navedenih restrikcija se u sličnom maniru može primeniti i na nivou filtracije [10] klijenta ili primaoca, ukoliko to zahteva koncept konfiguracija MTA.

6. Podešavanje sistema, otklanjanje grešaka i bagova, upotrebom Syslog i Round-Robin alata

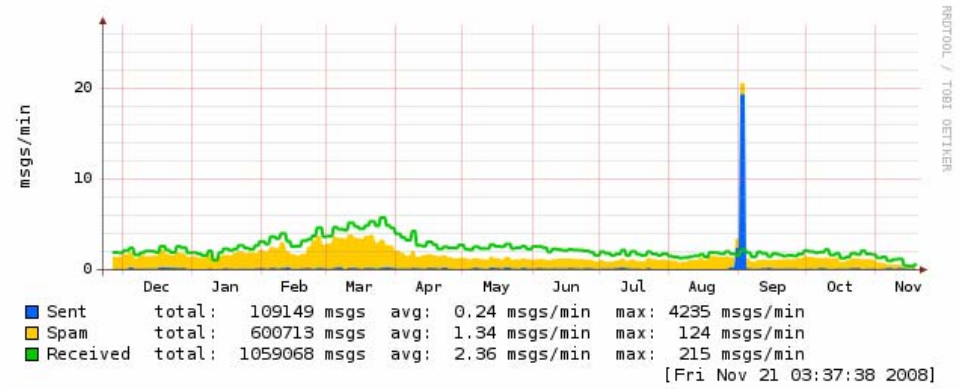
Monitoring rada *e-mail* servisa se smatra nezaobilaznim segmentom aktivnosti u procesu detekcije i analize potencijalnih problema, kao i kod praćenja rezultata prilikom implementacije novih rešenja.



Slika 3. *Grafička interpretacija prikupljenih podataka na e-mail serveru*

Syslog servis [11] je jedan od najvažnijih i najčešće korišćenih *logging* servisa kod sistema baziranih na UNIX-u. Jedna od najvažnijih osobina ovog servisa je potpuna kompatibilnost sa Postfix-om, čime se pruža mogućnost praćenja procesiranja jedne poruke do najsitnijih detalja, ali i mogućnost podešavanja nivoa detaljnosti informacija koje se preuzimaju. Direktan pregled *log* datoteka je pogodan za dijagnostičke postupke, ali ne u potpunosti i za praćenje sistema u celini. Navedeni problem se može rešiti uvođenjem grafičke interpretacije aktivnosti MTA, što je omogućeno upotrebom alata zasnovanim na Round-Robin principu rada, poput Mailgraph-a [12], koji koristi RRDTool. Osnovna osobina RRDTool alata [13] je formiranje statistike na bazi evidentiranog događaja u okviru definisanog vremenskog intervala. Na taj način se formira *rrd* statistička datoteka koja se nadalje koristi za formiranje grafičke interpretacije prikupljane statistike, slika 3.

U primeru koji je prikazan u ovom radu, analiza rada *e-mail* servera se vrši upotrebom navedenih alata. Rad sistema u celini se prati preko statistike broja primljenih, odbijenih i poslatih *e-mail* poruka, kao i broja poruka koje su identifikovane kao spam od strane programa SpamAssassin i broja poruka koje su prepoznate, od strane antivirusnog programa, kao poruke zaražene virusom. U slučaju posmatranog sistema, koristi se antivirusna zaštita Kaspersky Antivirus for Linux Mail Servers 5.5. Statistika se formira na dnevnom, nedeljnom, mesečnom i godišnjem nivou. Vrednosti koje su predstavljene u svim vremenskim presecima su: ukupan broj poruka, prosečan broj poruka u minuti, kao i maksimalan broj poruka u minuti, slika 4.



Slika 4. *Slučaj bezbednosnog propusta u konfiguracijiPostfixMTA i SpamAssassin-a*

Metodologija praćenja rada *e-mail* servera može zavisiti od veličine sistema koji se opslužuje, kao i od obima i važnosti komunikacije koja se ostvaruje ovim putem. Grafička interpretacija prikupljene statistike je pogodna i za uočavanje potencijalnih problema u radu. Primer naveden na slici 4. je ukazao na neuobičajeno visok intenzitet slanja poruka u trajanju od nekoliko časova, a detaljna analiza *log* datoteka, koja je zatim usledila, pokazala je da je došlo do eksploatacije bezbednosnog propusta u konfiguraciji SpamAssassin-a i Postfix-a, od strane spamera, koji su u datom slučaju koristili navedeni propust za serverski *relaying*. Propust je eksploatisan u trajanju od 2 časa i 20 minuta i za to vreme je propušteno ukupno oko 72.300 *e-mail* poruka.

```
oct 21 04:37:43 sf postfix/smtpd[5318]: connect from gqp76-1-87-89-28-76.dsl.club-internet.fr[87.89.28.76]
oct 21 04:37:46 sf postfix/smtpd[5318]: 156C8BC08F: client=gqp76-1-87-89-28-76.dsl.club-
internet.fr[87.89.28.76]
oct 21 04:37:46 sf postfix/cleanup[5404]: 156C8BC08F: message-
id=<140932103.84744698764107@bnds.com>
oct 21 04:37:46 sf postfix/qmgr[9174]: 156C8BC08F: from=<jhy@bnds.com>, size=1249, nrcpt=1 (queue
active)
oct 21 04:37:46 sf spamd[5117]: spamd: connection from localhost [127.0.0.1] at port 3167
oct 21 04:37:46 sf spamd[5117]: spamd: processing message <140932103.84744698764107@bnds.com> for
p.zdravkovic:1304
oct 21 04:37:47 sf spamd[5117]: spamd: identified spam (10.5/5.0) for p.zdravkovic:1304 in 0.3 seconds, 1249
bytes.
oct 21 04:37:47 sf spamd[5117]: spamd: result: Y 10 -
BAYES_60,FH_HELO_EQ_D_D_D_D,HELO_DYNAMIC_HCC,HELO_DYNAMIC_IPADDR,HTML_MESSAGE,
MIME_HTML_ONLY,RDNS_DYNAMIC
scantime=0.3,size=1249,user=p.zdravkovic,uid=1304,required_score=5.0,rhost=localhost,raddr=127.0.0.1,rpor
t=3167,mid=<140932103.84744698764107@bnds.com>,bayes=0.607904,autolearn=spam
oct 21 04:37:47 sf spamd[5108]: prefork: child states: II
oct 21 04:37:47 sf postfix/pipe[5405]: 156C8BC08F: to=<p.zdravkovic@sf.bg.ac.yu>, relay=spamfilter,
delay=1.4, delays=1/0.01/0/0.38, dsn=2.0.0, status=sent (delivered via spamfilter service)
oct 21 04:37:47 sf postfix/qmgr[9174]: 156C8BC08F: removed
oct 21 04:37:47 sf postfix/pickup[5155]: 474B7BC091: uid=1079 from=<jhy@bnds.com>
oct 21 04:37:47 sf postfix/cleanup[5404]: 474B7BC091: message-
id=<140932103.84744698764107@bnds.com>
oct 21 04:37:47 sf postfix/qmgr[9174]: 474B7BC091: from=<jhy@bnds.com>, size=4015, nrcpt=1 (queue
active)
oct 21 04:37:47 sf postfix/smtpd[5423]: connect from localhost[127.0.0.1]
oct 21 04:37:47 sf postfix/smtpd[5423]: 689CDBC08F: client=localhost[127.0.0.1]
oct 21 04:37:47 sf postfix/cleanup[5404]: 689CDBC08F: message-
id=<140932103.84744698764107@bnds.com>
oct 21 04:37:47 sf postfix/qmgr[9174]: 689CDBC08F: from=<jhy@bnds.com>, size=4334, nrcpt=1 (queue
active)
oct 21 04:37:47 sf postfix/smtpd[5423]: disconnect from localhost[127.0.0.1]
oct 21 04:37:47 sf postfix/lmtp[5419]: 474B7BC091: to=<spamcontainer@sf.bg.ac.yu>,
orig_to=<spamcontainer>, relay=127.0.0.1[127.0.0.1]:10030, delay=0.2, delays=0.01/0.01/0.03/0.15,
dsn=2.0.0, status=sent (250 2.0.0 <spamcontainer@sf.bg.ac.yu> Ok)
oct 21 04:37:47 sf postfix/qmgr[9174]: 474B7BC091: removed
oct 21 04:37:47 sf postfix/local[5424]: 689CDBC08F: to=<spamcontainer@sf.bg.ac.yu>, relay=local, delay=0.1,
delays=0.05/0.01/0/0.04, dsn=2.0.0, status=sent (delivered to mailbox)
oct 21 04:37:47 sf postfix/qmgr[9174]: 689CDBC08F: removed
```

Slika 5. *Prikaz log datoteke formirane pomoću syslog servisa*

Gruba analiza *log* datoteke (slika 5.) ukazala je na izvorišnu IP adresu napada, koja je odmah blokirana na *firewall*-u, nakon čega je usledila i detaljna analiza, koja je otkrila i pojedinosti vezane za sam propust (u datom slučaju – *read/write* pravo korisnika na objektu za koji navedeno pravo sme imati samo *root* korisnik). Propust je, naravno, ubrzo i uklonjen.

7. Poboljšanje rezultata

Efikasnost anti-spam sistema, u određenim slučajevima, može zavisiti od interakcije korisnika *e-mail* servisa sa sistemom. Mogući su slučajevi kada samo nekoliko (od par hiljada) korisnika dobije spam poruku, koja je poslata sa legitimne adrese (javni *webmail* servis), što znači da navedena poruka nema statističku važnost sa stanovišta sistema, kao ni neke druge atribute, da bi automatski bila pozitivno identifikovana. Ali, ona je za krajnjeg primaoca i dalje - neželjena poruka.

U slučajevima poput navedenog je bitno "naučiti" sistem, a da to predstavlja jednostavan korak za krajnjeg korisnika, koji predstavlja činioca koji može da utiče na proces "treninga" čitavog sistema.

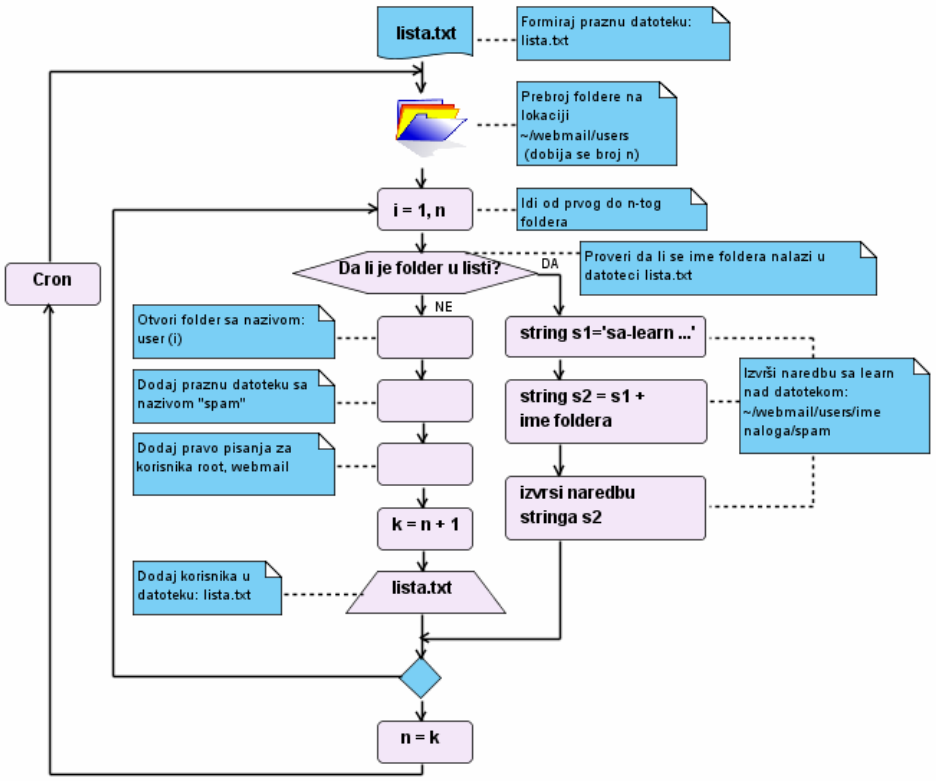
Sistem, koji se posmatra u ovom radu, je baziran na OpenSUSE Linux platformi, sa Postfix MTA, SpamAssassin anti-spam zaštiti, Kaspersky antivirusnom

rešenju, RRDTools i Mailgraph monitoringu, kao i NeoMail webmail programu. Sistem opslužuje 891 korisnika. SpamAssassin je integrisan na način predstavljan na slici 1.

Statistika pokazuje da je, u posmatranom 24-časovnom periodu, u sistem ušlo 3923 zahteva za isporuku pošte, od kojih je 3218 odbačeno na osnovu seta restrikcija na Postfix-u, 70 na osnovu identifikacije SpamAssassin-a i 9 na osnovu identifikacije virusa u sadržaju poruke. Ukupno je 626 poruka ušlo u sistem. Detaljnim analizama *log* datoteka je utvrđeno da je u sistem ušlo 116 spam poruka, što predstavlja 2.95% od ukupne količine dolazne pošte. Dakle, prosek po korisniku iznosi 0.57 pisama korisne sadržine i 0.13 spam pisama. Prosek za spam poruke u slučaju nebranjenog sistema je 3.83 poruke po korisniku.

Potreba za poboljšanjem navedenih rezultata potiče od činjenice da spam poruke nisu ravnomerno raspoređenje po destinacionim adresama, odnosno visoka je verovatnoća da će jedan korisnik dobiti i do 15 spam poruka, dok drugi korisnici neće primiti ni jednu poruku ovog tipa.

Zbog navedenih razloga predlaže se sledeće rešenje. NeoMail platforma za *webmail* servis ima mogućnost formiranja korisničkih foldera za klasifikaciju pošte, odnosno, postoji mogućnost izmeštanja poruka iz *inbox* foldera u novi folder. Struktura ovog foldera na nivou fajl sistema je, u stvari, datoteka koja sadrži navedene poruke, a čija je fizička struktura identična strukturi *inbox*-a, slika 6.



Slika 6. *Algoritam implementacije mehanizma za "učenje"*

SpamAssassin ima mogućnost "učenja" na osnovu jednog uzorkovanog pisma ili na osnovu kompletnog sadržaja *mailbox*-a korisnika, pod uslovom da se u njemu nalaze isključivo spam poruke.

Predloženo rešenje upravo koristi činjenicu da se "učenje" može izvesti na osnovu kompletnog sadržaja *mailbox*-a, pri čemu se u odgovarajućoj naredbi koristi fizička adresa *mailbox* datoteke (*sa-learn --no-sync --spam --mbox ~/userinbox*).

Predloženo rešenje predstavlja, u stvari, skript koji ima zadatak da, automatski na svakih sat vremena (ili drugi definisani period), u prvoj fazi, automatski postavi folder (datoteku) sa imenom *spam* (ukoliko već ne postoji) u svaki od *webmail* naloga, a zatim da, u drugoj fazi, izvršava komandu "učenja" nad svakom od postavljenih datoteka. Za navedenu svrhu bi se koristio *Cron* servis čija je funkcija izvršavanje programa u definisanim vremenskim intervalima.

Prethodno predstavljeni rezultati se samo delimično mogu uporediti sa rezultatima konfiguracija predstavljenih u [14, 15]. Razlog za navedenu nemogućnost detaljnije komparacije je različitost okruženja u kome se vrše merenja.

Prva konfiguracija (A) sadrži komponente Postfix, AmawisD-New, ClamAV i Spam Assassin koje su postavljene na Mandrake (Mandriva) platformi. Rezultati koji su vezani za ovu konfiguraciju su delimično precizni i na 24-časovnom nivou imaju sledeće vrednosti: u sistem je ušlo 6033 poruke, od kojih je 4723 odbijeno upotrebom filtera, a zatim još 403 klasifikovano kao Spam od strane SpamAssassin filtera, dok je učešće spam poruka u ukupnoj masi poruka koje su prošle ka korisnicima oko 50%, prema proceni autora, pri čemu se ne navodi ukupan broj korisnika. To znači da je procenjena količina spam poruka koja je prošla zaštitni sistem oko 7,5%, dok je količina detektovanog spama oko 85%, tabela 1.

Proizvod	Procenat identifikovanog spama	Procenat spama koji je ušao u sistem (false negatives)
Predložena konfiguracija	86,9%	2,95%
Konfiguracija A	85%	7,5%

Tabela 1. *Komparacija efikasnosti na osnovu procenta identifikovanog spama* [14]

Naredna komparacija (tabela 2.) nije mogla biti inkorporirana u prethodnu (tabela 1.) pošto autori sledećeg testa nisu uključivali DNS filtraciju.

Proizvod	Spam	Mogući spam	Spam koji je prošao u sistem (*false negatives*)
SpamAssassin (konfiguracija A)	66%	n/a	44%
M-Switch Anti-Spam (konfiguracija B)	81%	9%	5%

Tabela 2. *Komparacija efikasnosti na osnovu procenta identifikovanog spama bez prisustva DNS filtera* [15]

Druga konfiguracija (B) je napravljena zbog poređenja SpamAssassin filtera, koji je besplatan, sa M-Switch Anti-spam programom, koji spada u grupu komercijalnih softvera. Rezultat ove komparacije je predstavljen u tabeli 2. Može se zaključiti da komercijalno rešenje daje bolje rezultate u slučajevima kada je isključena filtracija na *smtpd* serveru. U slučaju uključenja navedene filtracije predložena konfiguracija značajno

poboljšava rezultat, pri čemu tada postoji veća verovatnoća da dođe do odbacivanja *e-mail* poruka sa korisnim sadržajem, odnosno da dođe do diskvalifikacije poruka zbog neregularno konfigurisanog izvorišnog servera (nepravilan *helo*, itd.).

8. Zaključak

Pravovremena i odgovarajuća reakcija administrativnog osoblja zavisi od prilagođenosti interfejsa za nadzor značajnih parametara sistema. Od njihove reakcije zavisi verovatnoća pojave domena datog sistema na *gray* ili *black* listama.

Treniranje anti-spam sistema od strane korisnika može dodatno pospešiti uspeh pri detekciji spam poruka u slučaju kada korisnici *e-mail* servisa poseduju zadovoljavajući stepen agilnosti da pri svakodnevoj upotrebi odmah klasifikuju poruke na korisnu poštu ili spam. Predloženo rešenje može biti prošireno i mehanizmom za "pozitivnu" identifikaciju poruka koje su pre toga pogrešno identifikovane kao spam (*false positives*), pri čemu takvo rešenje zahteva prisutstvo naloga koji bi imao ulogu spam kontejnera.

Literatura

[1]http://www.sophos.com/pressoffice/news/articles/2008/07/dirtydozjul08.html, (28.10.2008.)
[2] http://www.webopedia.com/TERM/s/spam.html, (28.10.2008.)
[3] http://spam.abuse.net/overview/whatisspam.shtml, (28.10.2008.)
[4] http://www.spamhaus.org/definition.html, (28.10.2008.)
[5] http://en.wikipedia.org/wiki/E-mail_spam, (28.10.2008.)
[6] DH. Shih, HS. Chiang, B. Lin, "Collaborative spam filtering with heterogeneous agents", *Expert Systems with Applications,* Vol. 35, 2008, pp. 1555–1566.
[7] http://wiki.apache.org/spamassassin, (28.10.2008.)
[8] http://www.postfix.org/documentation.html, (29.10.2008.)
[9] http://jimsun.linxnet.com/misc/postfix-anti-UCE.txt, (29.10.2008.)
[10] M.N. Marsono, et al, "A spam rejection scheme during SMTP sessions based on layer-3 e-mail classification", *Journal of Network and Computer Applications, article in press,* Vol. 32, 2009, pp. 236-257.
[11] http://www.syslog.org/syslog-ng/v2, (29.10.2008.)
[12] http://mailgraph.schweikert.ch, (29.10.2008.)
[13] http://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html, (29.10.2008.)
[14] http://mandrivausers.org/lofiversion/index.php/t37222.html, (29.10.2008.)
[15] http://www.isode.com/whitepapers/spamassassin-benchmark.html, (29.10.2008.)

Abstract: *E-mail server and client security has became highly dependent on antispam protection system. This paper represents a technical solution for improvement of antispam protection system on servers based on Postfix MTA.*

Keywords: *Antispam protection, SpamAssassin, Postfix, SMTP, Mailgraph, Monitoring*

AN IMPROVEMENT OF ANTISPAM MODEL IMPLEMENTATION

Snežana Mladenović, Slobodan Mitrović, Slađana Janković