HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Zaštita od neželjenih poruka verifikacijom adresa (SAV)

CCERT-PUBDOC-2007-08-200

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

Neželjene poruke elektroničke pošte (eng. *spam*, *junk e-mail*, *bulk e-mail*) danas su svakodnevna pojava koja stvara sve više neugodnosti korisnicima računala i zadaje sve više problema službama održavanja poslužitelja. Iako je njihovo korištenje bilo nezakonito još od početaka Interneta, one se pojavljuju u sve većim količinama. Istraživanja pokazuju da danas oko 85% svih poruka čine neželjene (90 milijardi poruka na dan). Budući da primanje takvih poruka ne uzrokuje samo neugodnosti, već dovodi i do problema sa zagušenjem poslužitelja i podatkovnih veza, nije čudno da industrija ulaže mnogo novca u borbu protiv njih. Dosadašnji rezultati tih ulaganja su uglavnom alati koji se temelje na filtriranju neželjenih poruka (eng. *spam filter*). Takvi filtri uglavnom sadrže kompleksne algoritme za analizu sadržaja poruke na osnovu kojeg određuju je li određena poruka neželjena ili ne. Međutim, autori neželjenih poruka se brzo prilagođavaju i novim metodama često uspijevaju zavarati filtre. Stoga se u novije vrijeme sve češće pribjegava drugoj vrsti zaštite od neželjenih poruka - SAV (eng. *Sender Address Verification*) zaštiti. Ona se temelji na verifikaciji adrese pošiljatelja interakcijom s njegovim poslužiteljem elektroničke pošte. Samo u slučaju uspješne verifikacije poruka se isporučuje u poštanski sandučić primatelja. U nastavku dokumenta prikazani su detaljniji opis SAV metode zaštite od neželjenih poruka kao i primjer njene implementacije na Postfix poslužitelju. Osim toga, napravljen je i kratak pregled ostalih metoda zaštite temeljenih na filtriranju poruka.

# 2. Problem neželjene pošte

Iako običnom korisniku neželjene poruke predstavljaju samo neugodnost, administratorima sustava one predstavljaju stvaran problem koji za njih znači i stvaran trošak. Slanje neželjenih poruka ne predstavlja velik trošak za njihovog autora, ali njihovo primanje, obrađivanje i pohranjivanje predstavlja velik trošak za sustav primatelja. Analize su otkrile da je 2003. godine zbog neželjenih poruka gospodarstvo Sjedinjenih Država izgubilo oko 10 milijardi dolara. Baš zbog takvih posljedica u većini zemalja doneseni su zakoni o sankcioniranju slanja neželjenih poruka, pa se njihovi autori danas uglavnom nalaze u slabije razvijenim zemljama gdje im je teže ući u trag. Istraživanjem je utvrđeno da gotovo 80% neželjenih poruka dolazi iz samo 600 izvora.

Unatoč tome što je slanje neželjenih poruka u većini zemalja ilegalno, takve poruke nisu iskorijenjene. Naime, provođenje zakona o zabrani neželjenih poruka ovisi o davateljima usluga Internet pristupa koji u velikom broju slučajeva nisu dovoljno dobro tehnički opremljeni za provođenje zakona ili pak ne žele provoditi zakon jer bi se time morali odreći klijenata koji im donose mnogo novca.

Drugi problem u suzbijanju neželjenih poruka su loše definirani zakoni kao što je američki CAN-SPAM Act iz 2003. godine koji dozvoljava reklamne poruke ako zadovoljavaju određene uvjete. Jedan od njih je mogućnost odbijanja daljnjeg primanja poruka iz izvora koji ih šalje. Međutim poznato je da autori neželjenih poruka koriste zahtjeve za odbijanje daljnjeg primanja samo kao potvrdu da su poslali poruku na važeću adresu elektroničke pošte. Time taj zakon postaje kontraproduktivan jer korisnici koji su svjesni ove opasnosti neće ni pokušati poslati zahtjev za odbijanje daljnjeg primanja čak i ako on nije lažan, dok će oni neiskusniji uvijek slati zahtjeve za odbijanje i tako davati informacije autorima neželjenih poruka. Istraživanje iz 2002. godine pokazalo je da 16% stranica na koje je poslan zahtjev za odbijanjem daljnjeg primanja poruka ignoriraju taj zahtjev i nastavljaju slati poruke na istu adresu.

## 2.1. Vrste neželjene pošte

Budući da se neželjena pošta koristi za reklamiranje, provedeno je istraživanje da bi se utvrdilo što se najčešće reklamira neželjenim porukama. Rezultati su prikazani u slijedećoj tablici.

| Vrsta reklame | Postotak |
|---|---|
| Proizvodi | 25 % |
| Financije | 20 % |
| Proizvodi za odrasle | 19 % |
| Prevare | 9 % |
| Zdravlje | 7 % |
| Internet | 7 % |
| Zabava | 6 % |
| Duhovnost | 4 % |
| Ostalo | 3 % |

**Tablica 1.** Zastupljenost neželjenih poruka prema području koje reklamiraju

Iz tablice je vidljivo da, unatoč tome što su najuočljivije, neželjene poruke o proizvodima za odrasle čine tek 19 % ukupne količine neželjenih poruka.

## 2.2. Principi rada autora neželjenih poruka

Tri su osnovna principa rada autora neželjenih poruka:

- anonimnost – kreiranje lažnih *e-mail* korisničkih računa tako da se ne može ući u trag njihovim vlasnicima,
- automatizacija – korištenje računala (poslužitelja elektroničke pošte) za generiranje i automatsko slanje velike količine poruka u kratkom vremenu, te
- mentalitet utrke u naoružanju – slanje sve više i više poruka kako bi se osigurala jednaka količina uspješno proslijeđenih poruka, neovisno o poboljšanjima filtara za njihovo uklanjanje.

### 2.2.1. Anonimnost

Uobičajena praksa autora neželjenih poruka je kreiranje korisničkih računa kod davatelja besplatnih *webmail* usluga. Za to nije potrebna verifikacija identiteta, a takvi se računi mogu koristiti za slanje neželjenih poruka i za primanje poruka od potencijalnih naručitelja. Budući da je potrebno odaslati velik broj poruka autori obično kreiraju nekoliko korisničkih računa i onda koriste alate za automatizirano slanje poruka s njih.

Davatelji *webmail* usluga zaštićuju se od automatiziranog kreiranja korisničkih računa postavljanjem dodatnog upita prilikom kreiranja računa. Upit se sastoji od grafičkog prikaza nekoliko izobličenih ali još uvijek čitljivih slova koja korisnik mora ručno unijeti u formu (tzv. captcha – od eng. *capture*). Takva slova nisu strojno čitljiva pomoću standardnih OCR (eng. *Optical Character Recognition* – prepoznavanje slova prilikom skeniranja) alata pa se kreiranje korisničkog računa ne može automatizirati.

Međutim, autori neželjenih poruka su i tome doskočili. Postoje dojave o stranicama na kojima autori poruka nude besplatne pornografske sadržaje za pristup kojima korisnik mora unijeti slova koja se prikazuju na formi za kreiranje webmail korisničkog računa. Nakon unosa slova autor neželjene poruke praktički dobiva automatizaciju kreiranja korisničkog računa, a korisnik dobiva besplatan pristup pornografskom materijalu.

Druga metoda za postizanje anonimnosti je korištenje tuđih računala. Naime ako autori neželjenih poruka koriste istog davatelja usluga za slanje velikog broja poruka prije ili kasnije će davatelj usluga to uočiti i vrlo brzo onemogućiti. Zbog toga autori neželjenih poruka pribjegavaju drugoj metodi – preuzimanju kontrole nad tuđim računalima i njihovom korištenju za slanje neželjenih poruka. Budući da je danas, pojavom ADSL-a i kabelskih veza, broj računala koja su stalno povezana na Internet postao ogroman, povećao se i broj nedovoljno zaštićenih računala povezanih na Internet. Na takva računala autori neželjenih poruka ubacuju zlonamjerno oblikovane programe koji šalju automatizirane poruke bez znanja korisnika. Tako su autori osigurali način za slanje velikog broja poruka koji će ih izmaknuti iz dohvata zakona.

Jedna od metoda koju su autori često koristili u 1990-ima bilo je slanje poruka putem tzv. *open – relay* poslužitelja. To su standardni poslužitelji elektroničke pošte konfigurirani tako da prosljeđuju svaku dobivenu poruku prema njenom odredištu bez obzira na identitet izvora poruke. Budući da je u 1990-ima takva konfiguracija bila uobičajena autori neželjenih poruka imali su mnogo mogućnosti za njihovu distribuciju. Izmjenom SMTP standarda došlo je do promjena u uobičajenoj konfiguraciji poslužitelja pa je današnji broj *open – relay* poslužitelja relativno malen.

Korištenju *open – relay* poslužitelja slično je korištenje tzv. *open proxy* poslužitelja za distribuciju neželjenih poruka. Posredni poslužitelj (eng. *proxy*) je poslužitelj koji nudi uslugu ostvarenja neizravnih veza na druge usluge. Ukoliko ga koristi, klijent se poveže na posredni poslužitelj koji se zatim povezuje prema ciljnom poslužitelju. Kada se veza uspostavi ciljni poslužitelj nije svjestan stvarnog klijenta, već je za njega klijent posredni poslužitelj. Usluge posrednog posluživanja imaju široko područje primjene pa se između ostalog koriste i za privremeno pohranjivanje web stranica, filtriranje web sadržaja, zaobilaženje vatrozida i sl. *Open proxy* je poslužitelj koji nudi uslugu posrednog posluživanja bez prethodne autentikacije klijenta te omogućava vezu na bilo koji poslužitelj. Autori neželjenih poruka spajaju se na *open proxy* poslužitelje kako bi putem njih mogli poslati neželjene poruke i kako im se pritom ne bi moglo ući u trag. Nakon što je ova pojava uočena broj *open proxy* poslužitelja je u stalnom padu.

Osim opisanih metoda jedna od često korištenih je i slanje neželjenih poruka putem nezaštićenih usluga. Primjer za to je `FormMail.pl` skripta koja se koristi kako bi se korisnicima web stranica omogućilo slanje povratne informacije o web stranici putem web forme. Neke inačice te skripte dozvoljavaju manipulaciju odredišne adrese poruke te se koriste za slanje neželjenih poruka. Takve poruke mogu se prepoznati po svojstvenom početku: "*Below is the result of your feedback form*".

### 2.2.2. Automatizacija

Trenutno u svijetu samo nekoliko tvrtki proizvodi aplikacije za slanje neželjenih poruka (eng. *spamware*). Takve aplikacije se poprilično razlikuju, ali njihove funkcionalnosti se uglavnom svode na učitavanje velikog broja adresa, njihovo slučajno generiranje, ubacivanje lažnih zaglavlja u poruke elektroničke pošte te simultano korištenje i iskorištavanje *open relay*, odnosno *open proxy*

poslužitelja. Treba napomenuti da je prodaja *spamware* aplikacija zakonom zabranjena u osam država SAD-a.

Kako bi se poslala neželjena poruka potrebno je doći do elektroničke adrese primatelja. Pribavljanjem adresa elektroničke pošte bave se autori neželjenih poruka, ali i trgovci adresarima. Prikupljanje adresa najčešće se odvija bez pristanka njihovih vlasnika ili čak unatoč njihovoj izričitoj zabrani, što dovodi do velikog broja neispravnih ili nevažećih adresa u tim popisima. Budući da autore neželjenih poruka slanje na velik broj adresa košta samo malo više nego slanje na mali broj adresa, količina nevažećih adresa ih ne brine previše te se često događa da poruke napisane primjerice na kineskom ili korejskom jeziku dolaze do ljudi koji ih uopće ne znaju pročitati.

Adrese se mogu prikupljati i na druge načine. Jedan od njih je korištenje alata koji pretražuju Internet i skupljaju adrese objavljene na web stranicama tvrtaka ili korporativnih adresara. Isto tako autori neželjenih poruka često se prijavljuju na razne forume kako bi dobili adrese njihovih ostalih sudionika. Drugi način prikupljanja adresa uključuje distribuciju tzv. *spam* virusa. On, jednom instaliran pretražuje korisničko računalo i kada pronađe adrese elektroničke pošte, popis šalje svom autoru.

Nakon što su pribavili adresu i iskoristili ju za slanje neželjene poruke, autori moraju provjeriti je li ta adresa uopće važeća. Jedan od načina provjere je posebno oblikovanje poslane poruke. Naime, ukoliko je poruka u HTML formatu, moguće ju je oblikovati tako da njeno otvaranje rezultira slanjem HTTP zahtjeva koji će potvrditi korisnikovu adresu.

Upotreba spam virusa i potonje opisane tehnike značajno je porasla prelaskom velikog broja korisnika na Windows XP operacijski sustav. On u svojoj inicijalnoj inačici sadrži nekoliko sigurnosnih propusta koji omogućuju kompromitiranje računala. Propusti su se zadržali čak i nakon izdavanja Service Pack 1 nadogradnje. Zanimljivo je da je i prethodna inačica Windows operacijskog sustava Windows 2000 imala jednake nedostatke, ali budući da ta inačica nije bila u širokoj upotrebi na kućnim računalima, nije bilo toliko mogućnosti za njihovo iskorištavanje. Podatak iz 2003. godine govori da je većina *e-mail* virusa te godine, uključujući i *Sobig* virus, bila korištena kao *spam* virus, tj. autorima su omogućavali korištenje zaraženog računala za slanje neželjenih poruka. Osim toga, zaražena su se računala koristila i za ostvarivanje DoS (eng. *Denial of Service*) napada na tvrtke i organizacije koje se bore protiv neželjenih poruka.

# 3. Filtriranje

Najčešća metoda obrane od neželjenih poruka je instalacija tzv. *spam filter* programa. To su alati koji se vežu na klijente elektroničke pošte ili na poslužitelje i presreću dolazne poruke kako bi utvrdili jesu li one željene ili neželjene. Ukoliko utvrde da se radi o neželjenoj poruci oni je ili zadržavaju ili je prosljeđuju korisniku s oznakom da se radi o neželjenoj poruci.

Filtriranje poruka temelji se na kompleksnim algoritmima koji implementiraju mehanizme umjetne inteligencije. Najčešće metode analize poruka temelje se na *Bayes*-ovom algoritmu ili na heurističkim algoritmima i, unatoč kompleksnosti, nijedna od primijenjenih metoda ne daje potpuno zadovoljavajuće rezultate u borbi protiv neželjenih poruka.

## 3.1. Metode

Filtriranje temeljeno na *Bayes*-ovom algoritmu zasniva se na vjerojatnostima pojavljivanja određenih riječi u (ne)željenim porukama. Na primjer, velik broj neželjenih poruka sadrži riječ „Viagra“ dok će se ista riječ rijetko naći u običnoj poruci. Filtar naravno ne zna vjerojatnost za svaku pojedinu riječ unaprijed već ga se mora trenirati da bi se došlo do vrijednosti vjerojatnosti koje će davati najbolje rezultate. Zbog toga korisnik mora u početku ručno odrediti je li neka pristigla poruka željena ili ne, a filtar će na osnovu njenog sadržaja prilagoditi granične vjerojatnosti pojedinih riječi kako bi se poruka pravilno klasificirala. Analizom većeg broja poruka raste baza poznatih riječi i fino se prilagođavaju njihove granične vjerojatnosti pa će tako nakon nekog vremena filtar dodijeliti vrlo visok koeficijent vjerojatnosti neželjene poruke za riječ „Viagra“, a vrlo nizak koeficijent vjerojatnosti neželjene poruke za imena korisnikovih prijatelja ili članova obitelji. Na osnovu koeficijenata riječi koje se nalaze u poruci pomoću *Bayes*-ovog izračuna dobiva se iznos ukupne vjerojatnosti da je poruka neželjena pa se sve poruke s iznosom većim od određenog praga automatski označavaju kao neželjene dok se druge propuštaju kao željene.

Heuristično filtriranje radi na sličnom principu – svaka pristigla poruka prolazi kroz nekoliko tisuća heurističkih pravila za analizu sadržaja, zaglavlja i okvira poruke na osnovu čega se izračunava vjerojatnost da je poruka neželjena. Dobivena vjerojatnost uspoređuje se s pragovima koje definira korisnik i na osnovu toga se poduzima određena akcija – poruka se briše, zahtijeva se ručna provjera ili se poruka prosljeđuje kao željena. Ova metoda međutim ima jednu veliku manu – baza heurističkih pravila se stalno mora obnavljati novim pravilima jer se autori neželjenih poruka vrlo brzo prilagođavaju postojećim pravilima i nalaze načine kako ih zaobići. Praksa također pokazuje da su baš zbog tog stalnog prilagođavanja alati koji se temelje na heurističkim provjerama prilično skloni pogreškama, što dovodi do značajnog broja lažno detektiranih neželjenih poruka.

## 3.2. Ograničenja

Dosadašnja iskustva pokazala su da alati za filtriranje neželjenih poruka imaju nekoliko vrlo značajnih mana:

- Filtri su osjetljivi na promjene na ulazu što autori neželjenih poruka iskorištavaju i to na dva načina:
  - Autorima neželjenih poruka bitan parametar je jedino količina „uspješnih“ neželjenih poruka. Što se više poruka detektira filtrima to će autori neželjenih poruka poslati više varijacija poruka da bi održali konstantan broj „uspješnih“ poruka.
  - U trenutku kad autori uoče neku manu u filtrima onda se vrlo brzo potrude maksimalno ju iskoristiti i u kratkom roku šalju velik broj odgovarajućih poruka.
- Filtri su ipak samo „umjetna inteligencija“ koju autori neželjenih poruka mogu zavarati na nekoliko načina:
  - Filtri traže specifične riječi u porukama pa autori neželjenih poruka u takve riječi ubacuju dodatna slova ili ih namjerno krivo pišu i to na način da su one još uvijek razumljive i čitljive čovjeku – npr. umjesto riječi *Viagra* često se pojavljuju riječi: *V1agra*, *Via'gra*, *V I A G R A*, *Vaigra*, *\/iagra*, *Vi@gra*. Istraživanja pokazuju da se korištenjem standardnih varijacija riječ „Viagra“ može napisati na 1,3 * $10^{21}$ načina.
  - Poruke u HTML formatu daju autorima neželjenih poruka još više mogućnosti za zavaravanje filtara - ubacivanje HTML komentara između slova riječi, ubacivanje teksta koji se ne vidi (zbog boje kojom je napisan) ili smanjivanje teksta na najmanju moguću veličinu mogu vrlo lako zavarati filtre.
  - Slanje teksta u obliku slike će gotovo sigurno zaobići filtar.
  - *Bayes*-ovo trovanje – metoda koju autori neželjenih poruka koriste za zavaravanje *Bayes*-ovih filtara. Temelji se na namjernom ubacivanju riječi koje se nikad ne koriste u neželjenim porukama u neželjene poruke čime se smanjuje mogućnost detekcije. Tako su nastale neželjene poruke koje u sebi sadrže odlomke iz raznih knjiga ili čak biblije čiji arhaičan stil gotovo sigurno uspijeva zavarati filtre.
  - Lažiranje adresa pošiljatelja umetanjem neke vjerodostojne domene ili cijele adrese može također zavarati filtre.
- Filtri su ili prestrogi ili preblagi – u namjeri da filtriraju što više neželjenih poruka proizvođači alata za filtriranje snižavaju pragove za detekciju neželjenih poruka što dovodi do velikog broja pogrešno detektiranih neželjenih poruka. To za posljedicu ima povisivanje pragova detekcije što opet dovodi do velikog broja nedetektiranih poruka. Konačan efekt je odustajanje od korištenja alata.

Zbog dosadašnjih iskustava filtri se lagano napuštaju i prelazi se na druge metode zaštite. Međutim, zbog velike količine novca uložene u postojeće alate korisnici pri kupnji novih moraju platiti i stare alate koji su sve manje efikasni.

# 4. SAV

Zbog svih navedenih nedostataka alati temeljeni na filtriranju poruka se sve više zamjenjuju drugim alatima i drugim metodama borbe protiv neželjenih poruka. Jedna od takvih je i metoda verifikacije adresa pošiljatelja poruke (eng. SAV – *Sender Address Verification*).

## 4.1. Princip rada

SAV metoda zaštite od neželjenih poruka temelji se na dodatnoj potvrdi identiteta nepoznatog pošiljatelja poruke. Sadržaj poruke je irelevantan – bitno je samo tko je pošiljatelj. Kada SAV sustav primi poruku od pošiljatelja od kojeg nikad prije nije primio poruku, on će mu odgovoriti porukom u kojoj se od njega zahtijeva potvrda identiteta putem neke jednostavne akcije. U većini slučajeva to znači odabir opcije *Reply* i slanje praznog odgovora, no radi zaštite od automatiziranih odgovora moguće je od pošiljatelja zahtijevati ručni unos grafički prikazanih znakova poslanih u zahtjevu za potvrdu. U trenutku kad je primljena potvrda SAV sustav prosljeđuje izvornu poruku primatelju, a pošiljatelju šalje obavijest o uspješnoj dostavi njegove poruke. Istovremeno SAV sustav obavještava pošiljatelja da je njegova adresa stavljena na listu verificiranih adresa i da buduće poruke pristigle s te adrese neće biti potrebno verificirati već će one biti izravno dostavljene primatelju.
SAV metoda zaštite skida veo anonimnosti s autora neželjenih poruka jer zahtjev za verifikaciju identiteta vodi natrag do pošiljatelja. Nije vjerojatno da će autori neželjenih poruka odgovarati na ove zahtjeve jer:

- su adrese pošiljatelja kod neželjenih poruka u velikoj većini slučajeva lažne i jer
- odgovorom na zahtjev za verifikaciju autor prihvaća odgovornost za slanje neželjene poruke.

## 4.2. Prednosti SAV sustava

U usporedbi sa zaštitom temeljenom na filtrima neželjenih poruka SAV zaštita ima nekoliko izrazitih prednosti:

- SAV reducira opterećenje poslužitelja elektroničke pošte i potrebne resurse za pohranjivanje poruka. Ako je SAV sustav implementiran kao samostalna aplikacija, obično je postavljen na rub mreže ispred infrastrukture za upravljanje elektroničkom poštom pa do poslužitelja dolaze samo poruke koje su verificirane SAV sustavom. Neželjene poruke nikad ne stignu do infrastrukture čime se izravno smanjuje opterećenje tih resursa. U nekim granama ljudske djelatnosti zakon propisuje pohranjivanje i indeksiranje svih primljenih poruka – uz SAV sustav koji ne prima neželjene poruke trošak pohranjivanja poruka je značajno smanjen.
- SAV nikad ne briše važeće *e-mail* poruke. *Spam* filtri koriste matematičke algoritme da bi odredili je li neka poruka neželjena ili ne. Koliko god ti algoritmi bili kompleksni, uvijek će se tu i tamo pojaviti greška i važeća poruka bit će označena kao neželjena. SAV sustavi nemaju tu manu jer ne izračunavaju koja je poruka neželjena već samo pitaju pošiljatelja da je verificira i time izbjegavaju pogreške.
- SAV reducira i količinu budućih neželjenih poruka jer razotkriva njihove autore. SMTP protokol kojim se ostvaruje komunikacija nema mehanizama za verifikaciju pošiljatelja poruke. Postoje tehnologije poput SPF (eng. *Sender Policy Framework*) ili *Domain Keys* koje to omogućuju, ali budući da nijedna od njih nije u širokoj upotrebi teško je ocijeniti njihovu efikasnost. SAV zaobilazi problem anonimnosti SMTP protokola tako da uopće ne analizira SMTP komunikaciju već anonimnost uklanja ili sa strane primatelja koji unaprijed definira listu važećih pošiljatelja ili sa strane pošiljatelja koji se mora identificirati da bi poruka bila primljena.

## 4.3. Predrasude o SAV sustavu

Iako je koncept SAV mehanizma zaštite prilično jednostavan mnogima je bilo nejasno kako ga implementirati i zbog toga su se pojavile neke predrasude o SAV metodi zašite:

1. SAV će udvostručiti promet elektroničke pošte zbog mnogih zahtjeva za verifikaciju. Pogreška u ovakvom razmišljanju je pretpostavka da će se za svaku poruku slati zahtjev za verifikaciju što nije točno iz dva razloga:
   a. Pošiljatelji se moraju verificirati samo prilikom slanja prve poruke dok će nakon toga svaka sljedeća poruka biti automatski dostavljena primatelju. Također, moguće je unaprijed definirati liste verificiranih primatelja pa pošiljatelji s tih lista uopće neće trebati verificirati svoj identitet.

   b. Autori neželjenih poruka često kao adresu pošiljatelja navode neku nevažeću adresu – pravilno implementirani SAV sustav može prepoznati takve adrese i za njih uopće ne generirati zahtjev za verifikaciju.
2. SAV sustavi će se međusobno zagušiti tzv. *ping pong* verifikacijskim zahtjevima. Srce svakog sustava za komunikaciju elektroničkom poštom je poslužitelj. Osnovna značajka svakog modernog poslužitelja elektroničke pošte je zaštita od tzv. zatvorenih petlji koje mogu nastati slanjem i primanjem poruka pa će shodno tome pravilno implementiran SAV sustav biti zaštićen od *ping pong* poruka.
3. SAV će blokirati važeće automatski generirane poruke (npr. poruke novinskih grupa). Dio svakog SAV sustava je red za čekanje u kojem se nalaze poruke koje čekaju odgovor na zahtjev za verifikaciju. Automatski generirane poruke bit će u tom redu, a SAV sustav dozvoljava administratorima da poruke iz tog reda sami verificiraju. Isto je omogućeno i pojedinim korisnicima za njihov red čekanja. Također neki SAV sustavi administratorima omogućuju definiranje cijele domene kao važećeg izvora poruka pa je tako moguće npr. definirati da sve poruke koje dolaze s adresa @amazon.com budu automatski proslijeđene primateljima bez verifikacije.
4. SAV je jednostavno zaobići lažiranjem adrese pošiljatelja tako da se zamijeni s nekom važećom adresom. Ova mogućnost postoji, ali time autori neželjenih poruka povećavaju svoj rizik jer se taj čin smatra zakonskom prijevarom, pa nije vjerojatno da će takvih poruka biti velik broj.

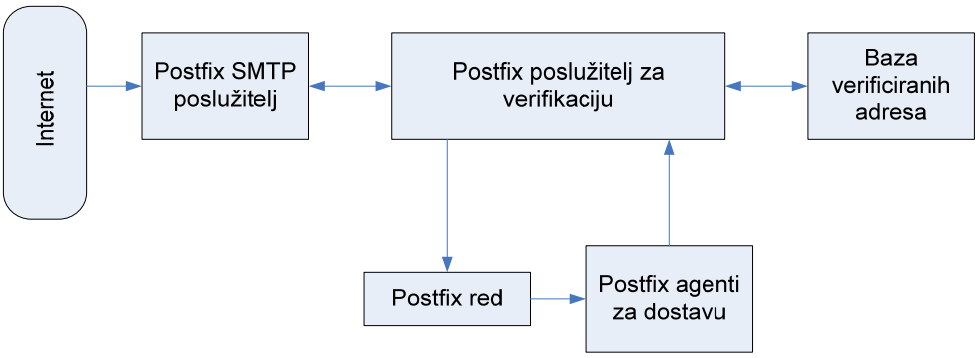
### 4.4. Nedostaci SAV sustava

Neželjene poruke i zaštitu protiv njih treba uvijek promatrati kao borbu dva natjecatelja. Stoga je kod dizajniranja sustava za zaštitu potrebno uvijek imati u vidu teoriju igara i pokušati predvidjeti reakciju autora neželjenih poruka na neku zaštitu. Prije uvođenja SAV sustava neželjene poruke su uglavnom bile slane s lažnim podacima o pošiljatelju i to je inicijalno učinilo SAV sustave efikasnim. Međutim nakon uvođenja SAV sustava, kako bi ga zaobišli, autori neželjenih poruka morali su kao pošiljatelje navoditi važeće adrese.

Prvo logično mjesto za pronalazak takvih adresa je popis adresa primatelja neželjenih poruka. Tako autori neželjenih poruka kao adresu pošiljatelja poruke navode adrese stvarnih ljudi kojima inače šalju neželjene poruke. Rezultat toga je slanje zahtjeva za verifikaciju poruke pa sada korisnici koji su inače pogođeni neželjenim porukama i nisu zaštićeni SAV sustavom dobivaju dvostruko više poruka – izvorne neželjene poruke i zahtjeve za verifikaciju dobivene zbog neželjenih poruka poslanih s njihovom adresom kao adresom pošiljatelja. Da bi se to spriječilo neki SAV sustavi kao što je npr. Postfix ne implementiraju potpuni mehanizam verifikacije adrese, već samo djelomičan. To znači da se verifikacijom ne zahtijeva direktna potvrda samog pošiljatelja poruke već se samo verificira postojanje adrese pošiljatelja putem komunikacije s e-mail poslužiteljem s kojeg adresa potječe. Na taj način smanjuje se promet vezan uz verifikaciju, ali se također smanjuje i efikasnost SAV sustava.

## 5. Primjer SAV sustava – Postfix

Postfix je jedan od poslužitelja elektroničke pošte koji podržava SAV metodu zaštite od neželjenih poruka. Princip rada sustava prikazan je na slici 1.




**Slika 1.** Postfix implementacija SAV zaštite

Kada sustav zaprimi poruku putem SMTP poslužitelja on inicira proceduru verifikacije adrese pošiljatelja. Zahtjev za verifikaciju obrađuje zaseban poslužitelj za verifikaciju koji prvo provjerava da li se adresa pošiljatelja već nalazi u bazi verificiranih adresa. Ako se ne nalazi šalje se zahtjev za verifikaciju u Postfix red iz kojeg Postfix agent za dostavu obrađuje jedan po jedan zahtjev. Postfix agent za dostavu šalje ispitni (eng. *probe*) zahtjev za verifikaciju i kad dobije odgovor obavještava poslužitelj za verifikaciju koji odgovor prosljeđuje SMTP poslužitelju. Tek kad dobije rezultat verifikacije, Postfix SMTP poslužitelj nastavlja s primanjem poruke ili je odbija primiti i šalje kod greške 450 ako verifikacija nije bila uspješna

Budući da se verifikacija obavlja ispitnim zahtjevom, cijeli proces ne bi trebao trajati duže od 6 sekundi, tj. razmak između trenutka kad Postifx SMTP poslužitelj počne primati poruku i trenutka kad taj poslužitelj nastavlja primati poruku ili je odbija primiti nije veći od 6 sekundi.

Ispitni zahtjev za verifikaciju u stvari je iniciranje SMTP sjednice s poslužiteljem bez samog slanja poruke, što znači da se za verifikaciju adrese ne zahtijeva odgovor samog pošiljatelja već samo potvrda postojanja njegove adrese. Time se u biti izbjegava izravno kontaktiranje pošiljatelja i utvrđivanje da li je on stvarno poslao tu poruku već se samo provjerava postojanje adrese pošiljatelja. Budući da se cijeli proces verifikacije obavlja automatski bez interakcije korisnika, može se obaviti brzo pa iz toga proizlazi i trajanje cijelog procesa od 6 sekundi ili manje.

Prilikom konfiguracije sustava poželjno je specificirati sljedeće:

- Listu domena za koje je potrebno raditi verifikaciju adresa – domene koje se često pojavljuju u neželjenim porukama. Poželjno je u te domene uključiti i vlastite domene. Nije poželjno uključiti verifikaciju za sve dolazne poruke jer će doći do gubitka poruka koje su odaslane s poslužitelja s kojima SAV sustav ne može uspostaviti uspješnu vezu za verifikaciju.
- Listu domena za koje nije potrebno raditi verifikaciju adresa – domena za koje se pouzdano može tvrditi da nisu izvor neželjenih poruka. Na ovu listu potrebno je staviti i sigurne domene koje koriste različitu adresu pošiljatelja za svaku poruku novinske grupe (npr. securityfocus.com) jer u suprotnom dolazi do nepotrebnog generiranja velikog broja zahtjeva za verifikaciju.

Bitno je znati da se po uobičajenim postavkama za bazu verificiranih adresa ne koristi trajno pohranjivanje, tj. podaci se ne pohranjuju na disk osim ako se to eksplicitno ne navede u konfiguraciji SAV sustava. Razlog za to je mogućnost da količina podataka preraste količinu slobodnog prostora na disku. Iako je moguće izmijeniti rok trajanja zapisa u bazi (koliko dugo se određena adresa drži u bazi ako nije korištena za verifikaciju) količina podataka u njoj može ponekad porasti.

## 5.1. Ograničenja Postfix SAV sustava

Zbog specifičnog načina implementacije Postfix SAV sustav ima i neka ograničenja:

- Za verifikaciju adrese Postfix šalje tzv. probe zahtjev najbližem agentu za prijenos poruka elektroničke pošte (eng. MTA – Mail Transfer Agent). Ispitni zahtjev ne uključuje slanje poruke već samo iniciranje SMTP sjednice korištenjem određene adrese. Ukoliko MTA prihvati danu adresu Postfix SAV sustav zaključuje da je adresa važeća što ne mora uvijek biti točno. Naime, moguća je situacija u kojoj bi prvi ili neki sljedeći MTA nakon najbližeg odbio zahtjev za daljnje prosljeđivanje poruke jer bi utvrdio da je adresa nevažeća.

- Postoji mogućnost da neki agenti za prijenos poruka počnu odbijati primanje ispitnih zahtjeva zbog njihovog prečestog slanja. Zbog toga bi trebalo koristiti verifikaciju adresa vrlo štedljivo ili je uopće ne koristiti u situacijama kad na sustav dolazi velik broj poruka.
- Obično verifikacija adresa ide istim putovima kao i slanje poruka, ali postoje i konfiguracije u kojima se poruke prema vanjskom svijetu šalju putem posrednog poslužitelja. U takvim konfiguracijama Postfix SAV sustav se mora posebno prilagoditi i postoji mogućnost da, ovisno o konfiguraciji, ne podržava potpunu funkcionalnost.
- Neki agenti za prijenos poruka ne javljaju poruku o nevažećoj adresi nakon ispitnog zahtjeva već tek nakon završetka prijenosa podataka SMTP protokolom šalju poruku o neuspjehu prijenosa. Postfix SAV sustav ne radi s takvim agentima.
- Po uobičajenim postavkama svi se ispitni zahtjevi šalju s `postmaster@$myorigin` adresom pošiljatelja. Ova postavka se može promijeniti čak i na način da adresa pošiljatelja bude prazna, ali treba imati u vidu da bi verifikacija adresa mogla biti neuspješna kod agenata koji ne prihvaćaju SMTP sjednicu ako je to polje prazno.

# 6. Zaključak

Vidljivo je, kako iz prikaza načina rada sustava zaštite temeljnih na filtrima, tako i iz iskustava s tim sustavima, da oni ne pružaju dovoljnu razinu zaštite od neželjenih poruka koliko god se pokušavali usavršiti. SAV predstavlja alternativu tim sustavima, ali nije ušao u širu upotrebu pa je teško ocijeniti njegovu efikasnost. Također vidljivo je da sustavi kao što je Postfix, koji jesu u upotrebi, ne implementiraju potpunu verifikaciju adresa koja uključuje i samu potvrdu korisnika već samo djelomičnu verifikaciju najbližeg agenta za prijenos poruka. Ta činjenica, potkrijepljena upozorenjem Postfix korisnicima da ne koriste SAV za verifikaciju u sustavima koji primaju puno poruka, govori da su korisnici i davatelji *e-mail* usluga ipak skloniji neinvazivnim metodama zaštite ne zahtijevaju izravnu interakciju korisnika ili izravnu potvrdu sustava pošiljatelja. Sudeći prema tome, problem neželjenih poruka još uvijek nije na razini zbog koje bi se podigla panika i uložilo više truda u njegovo sprečavanje.

# 7. Reference


[1] Heurističke metode filtriranja , http://www.spam-site.com/heuristic-spam-filter.shtml , kolovoz 2007.

[2] Bayes filtriranje, http://en.wikipedia.org/wiki/Bayesian_spam_filtering, kolovoz 2007.

[3] Spam općenito, http://en.wikipedia.org/wiki/E-mail_spam#Delivering_spam_messages, kolovoz 2007.

[4] SAV, http://www.circleid.com/posts/sender_address_verification_solving_the_spam_crisis/ , 2004.

[5] SAV, http://go.techtarget.com/r/1838191/4100818 , kolovoz 2007.

[6] SAV, http://taint.org/2007/03/16/134743a.html , kolovoz 2007.

[7] Postfix, http://www.postfix.org/ADDRESS_VERIFICATION_README.html , kolovoz 2007.