HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Sender Policy Framework

CCERT-PUBDOC-2006-02-148

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

SMTP (eng. *Simple Mail Transfer Protocol*) protokol [2] je standard za razmjenu elektroničke pošte koji dozvoljava da nominalna adresa pošiljatelja elektroničke pošte ne odgovara stvarnoj adresi s koje se pošta šalje. Većina *spamera* koristi tu činjenicu te kao pošiljatelja u *spam* porukama navode tuđe ili nepostojeće adrese.
Usmjeravanje korisničkih zahtjeva za odgovarajućim servisima domene (elektronička pošta, web, itd.) izvodi se korištenjem DNS (eng. *Domain Name Service*) poslužitelja. MX zapis (eng. *Mail Exchange record*) DNS poslužitelja registrira računalo koje prima elektroničku poštu za danu domenu. *Sender Policy Framework* (SPF) tehnologija temelji se na objavljivanju (u vidu DNS zapisa) reverznih MX zapisa koji označavaju računalo koje je namijenjeno slanju elektroničke poštu za danu domenu. Na taj način, poslužitelj elektroničke pošte koji primi poruku elektroničke pošte koja u `Return-Path` zaglavlju sadrži zapis oblika `adresa@domena.hr`, vjerodostojnost pošiljatelja provjerava jednostavnim DNS SPF upitom domeni `domena.hr`.
Dokument opisuje osnovna načela SPF tehnologije, implementaciju i glavne nedostatke SPF protokola te navodi neke od korisnika SPF tehnologije.

Slika 1: Oznaka domena koje implementiraju SPF protokol

2. Ideja SPF protokola

Neželjene poruke elektroničke pošte (eng. s*pam*) jedan su od najvećih problema računalnog svijeta. Autor ideje SPF tehnologije, Meng Weng Wong, navodi potrebu za promjenom paradigme elektroničke pošte [8], i to prema tablici *Tablica 1*:

Elektronička pošta u 20. stoljeću	Elektronička pošta u 21. stoljeću
Spam poruka je iznimka.	Većina poruka je *spam*.
Politika prihvaćanja poruka je „prihvati sve, odbaci neke“.	Politika prihvaćanja poruka je „odbaci sve, prihvati neke“.
Spam poruke evoluiraju te se lista razloga za odbacivanje poruka povećava.	Skup pošiljatelja pravih poruka elektroničke pošte je relativno statičan.
Filtriraj *spam* poruke na temelju njihovog sadržaja.	Propusti prave poruke na temelju pošiljatelja.
Potencijalnu *spam* poruku spremi u posebni direktorij, kojeg korisnik potom provjerava.	U poštanskom sandučiću korisnika nema *spam* direktorija.
Spam direktoriji smanjuju pouzdanost servisa, pošiljatelj ne zna je li poruka pročitana.	Ako je poruka prihvaćena, pošiljatelj je siguran da će biti pročitana.
Najteži zadatak borbe protiv *spam* poruka je smanjenje broja pravih poruka koje se klasificiraju kao *spam* poruke.	Ispravna klasifikacija poruka kao popratnu pojavu ima onemogućavanje *spam* poruka.
Nepoznati korisnici mogu istog trena izmjenjivati poruke.	Nepoznati korisnici moraju proći određen proces verifikacije.

Tablica 1: Usporedba elektroničke pošte u 20. i 21. stoljeću

Infrastruktura elektroničke pošte, definirana SMTP standardom, ne sadrži nikakav mehanizam autentifikacije korisnika. SPF je zamišljen kao nadogradnja na postojeći SMTP protokol, a moguće ga je ukratko opisati na sljedeći način:

1. Administrator domene, npr. `PrvaDomena.hr`, na svojem DNS poslužitelju objavi SPF zapis, određujući na taj način poslužitelje (računala) ovlaštene za slanje elektroničke pošte za tu domenu.
2. Poslužitelj elektroničke pošte za domenu `DrugaDomena.hr`, koji podržava SPF protokol, po primitku elektroničke pošte s domene `PrvaDomena.hr` odgovara slanjem DNS SPF upita. Na taj se način provjerava da li je adresa s koje je elektronička pošta stigla ovlaštena za slanje poruka za tu domenu.
3. Ukoliko postoji SPF zapis koji potvrđuje da je ta adresa ovlaštena za slanje elektroničke pošte za domenu `PrvaDomena.hr`, poslužitelj elektroničke pošte za domenu `DrugaDomena.hr` prihvaća pristiglu poruku. U suprotnom, pošta se odbacuje.

U svom radu SPF protokol štiti adresu navedenu u `Return-Path` zaglavlju poruke, odnosno adresu na koju se poruka vraća u slučaju nemogućnosti dostave. Ta adresa ne mora odgovarati adresi koja se nalazi u `From` odnosno `Sender` zaglavlju.

2.1. Uloga SPF protokola

Posljednjih se godina na različite načine pokušava povećati pouzdanost i vjerodostojnost SMTP protokola. Tri stavke koje sumiraju to nastojanje su:

- reputacija korisnika,
- akreditacija korisnika i
- autentifikacija korisnika.

Reputacija korisnika realizirana je javno dostupnim *blacklist* popisima koji navode provjerene pošiljatelje *spam* poruka. Na taj se način pošiljatelje *spam* poruka onemogućava da registriraju vlastitu domenu koja bi djelovala u skladu sa SPF protokolom.

Akreditacija korisnika realizirana je putem neovisnih organizacija koje garantiraju vjerodostojnost pošiljatelja. Primjeri takvih organizacija su Bonded Sender[4], ISIPP[5] i Habeas[6], akreditacijski sustavi koje koristi veliki broj servisa elektroničke pošte (Hotmail, MSN, RoadRunner i drugi).

Autentifikaciju korisnika moguće je realizirati upravo SPF protokolom, koji omogućava utvrđivanje da li je pošiljatelj poruke elektroničke pošte zaista onaj za kojeg se predstavlja. Autentifikacija pošiljatelja korisnicima donosi i druge beneficije. Na prvom mjestu to je nemogućnost da netko lažira njihovu adresu elektroničke pošte te im na taj način nanese štetu (tzv. „Joe-Job“ lažiranje). „Joe-Job“ postupak spada u kategoriju lažiranja sadržaja SMTP ovojnice (eng. *envelope*), odnosno `Return-Path` adrese, što SPF tehnologija u potpunosti onemogućava.
Drugi problem vezan uz autentifikaciju pošiljatelja su tzv. „phishing“ napadi. To su napadi koji lažiranjem izvora poruke od korisnika žele saznati osjetljive informacije, primjerice broj kreditne kartice. Primjer „phishing“ napada:

```
From: podrska@trgovina.hr
Subject: Problem s kreditnom karticom

Poštovani korisniče,
došlo je do problema s brojem Vaše kreditne kartice.
Molimo Vas da broj ponovno upišete na sljedeću adresu:
http://trgovina.hr@192.0.1.1/brojkartice.cgi
```

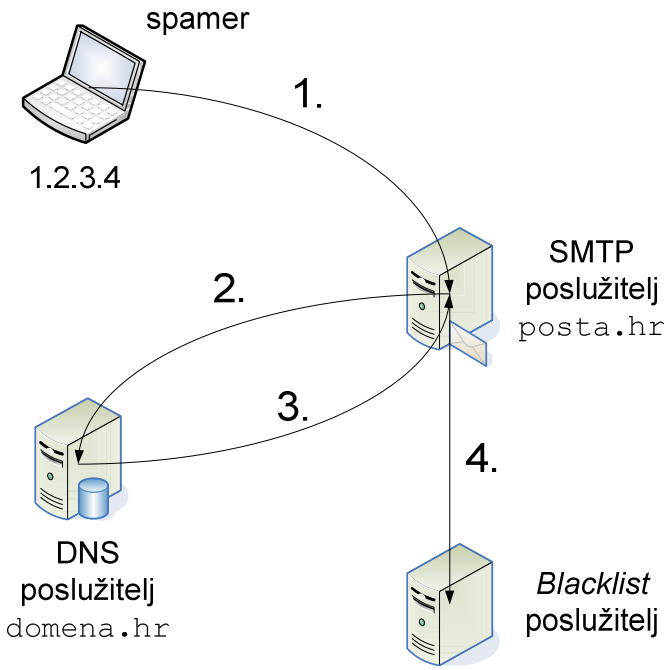
„Phishing“ napad temelji se na lažiranju sadržaja zaglavlja poruke elektroničke pošte, što je nemoguće spriječiti korištenjem SPF tehnologije. Ipak, za onemogućavanje opisanog napada postoje kriptografska rješenja u vidu digitalnog potpisa sadržaja (npr. PGP potpis), S/MIME ekstenzije ili Yahoo! DomainKeys tehnologije.

2.2. Ilustracija rada SPF protokola

Pretpostavimo da se elektronička pošta za domenu `domena.hr` uvijek šalje s IP adresa 161.53.64.0/24 i 205.12.16.0/24. Odgovarajući SPF zapis izgledat će ovako:

```
v=spf1 ip4:161.53.64.0/24 ip4:205.12.16.0/24 -all
```

U sljedećem dijagramu biti će prikazana komunikacija *spamera* koji pokušava poslati poruku korisniku domene `posta.hr`:



Slika 2: Pokušaj slanja *spam* poruke na SMTP poslužitelj koji koristi SPF protokol

Na početku pošiljatelj *spam* poruke, koji se nalazi na IP adresi 1.2.3.4, uspostavlja SMTP sjednicu s poslužiteljem elektroničke pošte za domenu `posta.hr`. Kao `Return-Path` navodi adresu oblika `korisnik@domena.hr` (faza 1).
SMTP poslužitelj `posta.hr` tada šalje SPF upit DNS poslužitelju za domenu `domena.hr` (faza 2). Budući da IP adresa 1.2.3.4 nije ovlaštena za slanje elektroničke pošte za domenu `domena.hr`, DNS poslužitelj vraća negativan odgovor, što rezultira odbacivanjem poruke pristigle s adrese 1.2.3.4 (faza 3).
Na kraju SMTP poslužitelj `posta.hr` može obavijestiti jedan ili više *blacklist* poslužitelja te na taj način onemogućiti pošiljatelja *spam* poruka u daljnjem djelovanju (faza 4).

3. Implementacija SPF protokola

3.1. Objavljivanje SPF zapisa

Termin „SPF zapis“ odnosi se na DNS RR (eng. *Resource Record*) zapis koji označava IP adrese računala ovlaštenih za slanje elektroničke pošte za danu domenu. Primjer SPF zapisa je sljedeći znakovni niz:

```
v=spf1 +mx +a:racunalo.domena.hr/28 -all
```

Ovaj SPF zapis označava korištenu inačicu SPF protokola (`spf1`) i tri direktive: „+mx“, „`+a:racunalo.domena.hr/28`“ te „-all“. Više o mehanizmima i direktivama u nastavku dokumenta.
Zapisi se objavljuju u vidu TXT DNS zapisa. Primjer objave za prethodni SPF zapis glasi:

```
domena.hr.   TXT   "v= spf1 +mx +a:racunalo.domena.hr/28 -all"
```

Domena ne smije imati višestruke SPF zapise koji bi prilikom autorizacijskog zahtjeva rezultirali odabirom više od jednog zapisa.

3.2. Mehanizmi i modifikatori

Domena koja implementira SPF protokol definira proizvoljni broj mehanizama koji se koriste za određivanje skupa računala ovlaštenih za slanje elektroničke pošte za danu domenu. Mehanizmi se koriste i za definiranje određenih aspekata sigurnosne politike elektroničke pošte (npr. sadržaj poruka elektroničke pošte je uvijek digitalno potpisan). Popis mehanizama je sljedeći:

- `a`
- `all`
- `mx`
- `ptr`
- `ip4`
- `ip6`
- `include`
- `exists`
- `extensions`

Domena može definirati i modifikator. Postoje dva modifikatora:

- `redirect`
- `explanation`

Pojašnjenje pojedinih mehanizama i modifikatora raspoloživo je u poglavlju 3.2.1. ovog dokumenta.
Mehanizmi kao prefiks mogu imati jedan od sljedeća četiri znaka:

- `-` (`fail`)
- `~` (`softfail`)
- `+` (`pass`)
- `?` (`neutral`)

Svaki prefiks definira akciju koju je potrebno provesti ukoliko je mehanizam evaluiran kao istinit. Ukoliko prefiks nije naveden, podrazumijeva se vrijednost „pass“. Prilikom evaluacije, mehanizmi se obrađuju redom kojim su navedeni. Ukoliko se neki mehanizam evaluira kao istinit, definirani prefiks određuje ukoliko je odgovarajuća IP adresa ovlaštena za slanje elektroničke pošte. Prefiks „fail“ označava da klijent nije ovlašten dok prefiks „pass“ označava da je klijent ovlašten za slanje poruka. Prefiks „neutral“ označava nemoćnost određivanje ovlasti klijenta dok prefiks „softfail“ predstavlja situaciju između „fail“ i „neutral“ odgovora u kojoj poslužitelj ne može sa sigurnošću potvrditi ovlasti klijenta.

3.2.1. Opisi mehanizama i modifikatora

Mehanizam "all" određuje sva računala bilo koje domene koja nisu prethodno prepoznata od drugih mehanizama. Stoga se mehanizam "all" smješta na kraj SPF zapisa. Uobičajeno se korištenjem drugih mehanizama definiraju legitimne IP adrese i klijenti ovlašteni za slanje poruka dok se „all“ stavlja uz prefiks „fail“ što znači da neprepoznate IP adrese i klijenti nisu ovlašteni za slanje poruka. Naravno, moguće je definirati i pojedinačne zabranjene IP adrese i klijente dok se svi ostali definiraju kao ovlašteni za slanje poruka stavljanjem prefiksa „pass“ uz mehanizam „all“.
Mehanizam „a“ provjerava sve adresne DNS zapise (A zapisi). Ukoliko se IP adresa klijenta koji je poslao poruku elektroničke pošte pronađe, mehanizam se evaluira kao istinit. Primjeri korištenja mehanizma:

```
a a:domena
a:domena/cidr-duljina
a/cidr-duljina
```

Ukoliko parametar domena nije specificiran, u evaluaciji se koristi trenutna domena (domena na kojoj se nalazi DNS poslužitelj). Parametar cidr-duljina koristi se za pretraživanje CIDR (eng. *Classless Inter-Domain Routing*) podmreže.
Prilikom evaluacije MX zapisa provjeravaju se svi odgovarajući adresni (A) zapisi. Ukoliko se tražena IP adresa nađe, mehanizam „mx“ se evaluira kao istinit. Primjeri korištenja:

```
mx mx:domain
mx:domain/cidr-duljina
mx/cidr-duljina
```

Naziv odnosno nazivi (moguće je definirati više naziva za istu IP adresu) računala na temelju njegove IP adrese određuje se iz odgovarajućeg PTR (eng. *Pointer Record*) DNS zapisa. Dobiveni nazivi se potom evaluiraju. Ukoliko barem jedan adresni (A) zapis za naziv dobiven PTR upitom odgovara IP adresi klijenta podvrgnutog SPF provjeri, mehanizam „ptr“ evaluira se kao istinit. Primjer korištenja:

```
ptr ptr:domain
```

Mehanizam „ip4“ koristi se za definiranje opsega adresa definiran CIDR adresnom shemom za IP protokol inačice 4 (IPv4). Analogno tome, opseg adresa definiran CIDR adresnom shemom za IP protokol inačice 6 (IPv6) definira se „ip6“ mehanizmom. Primjeri korištenja:

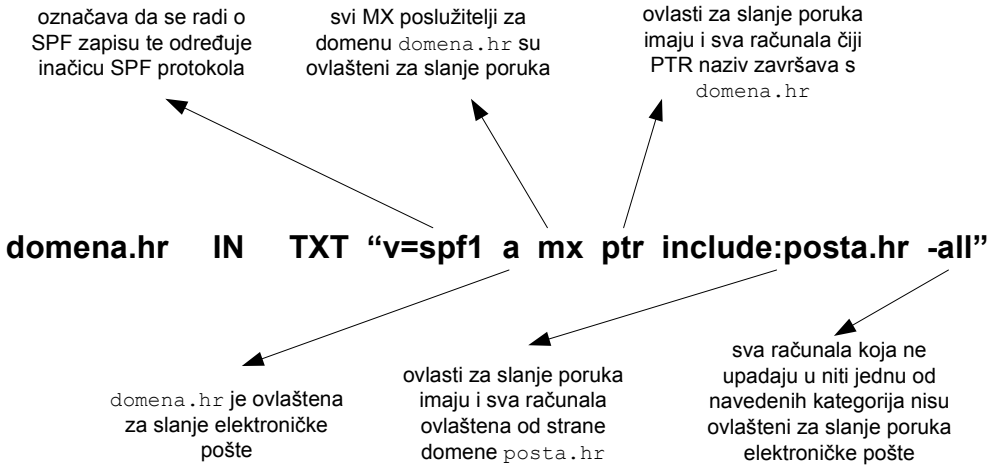
```
ip4:cidr-duljina
ip6:cidr-duljina
```

Mehanizam „exists“ kao argument prima adresu koja se proširuje na naziv domene. Dobiveni naziv koristi se u adresnom (A) DNS upitu. U slučaju da se odgovarajući zapis pronađe, mehanizam se evaluira kao istinit. Na taj način moguće je pojedinom korisniku (npr. korisnik@domena.hr) omogućiti slanje poruka elektroničke pošte s određene adrese (npr. 192.0.0.1).

Mehanizam „include“ koristi se u slučaju da se za slanje elektroničke pošte koriste poslužitelji koji se nalaze na drugoj domeni. Za ilustraciju postupka može poslužiti sljedeći SPF zapis:

```
”v=spf1 include:domena.net -all“
```

Ukoliko se za prethodni primjer provjerava IP adresa 1.2.3.4, a trenutna domena je domena.hr, DNS upit prosljeđuje se DNS poslužitelju za domenu domena.net.
Korištenje modifikatora je proizvoljno. Ukoliko se modifikator koristi, može se koristiti samo jednom po direktivi.
Modifikator „redirect“ sličan je „include“ mehanizmu, osim što se DNS zapis prosljeđuje drugoj domeni bez prethodne provjere trenutne domene. Modifikator „exp“ (explanation) omogućava dodavanje znakovnog niza koji pobliže opisuje pogrešku, u slučaju da dođe do iste.



Slika 3: Primjer SPF zapisa

Pseudo kod za primjer opisan na slici *Slika 3*:

```
ako(računalo pronađeno u A zapisima){ //a
   vrati „računalo je ovlašteno slati e-mail poruke“;
}inače ako(računalo pronađeno u MX zapisima){ //mx
   vrati „računalo je ovlašteno slati e-mail poruke“;
}inače ako(računalo pronađeno u PTR zapisima){ //ptr
   vrati „računalo je ovlašteno slati e-mail poruke“;
}inače ako(računalo je s domene posta.hr i ako ga poslužitelj
     ovlašten za tu domenu autentificira){ //include:posta.hr
   vrati „računalo je ovlašteno slati e-mail poruke“;
}inače(za sva računala){ //-all
   vrati „računalo nije ovlašteno slati e-mail poruke“;
}
```

4. Korisnici SPF tehnologije

SPF je danas implementiran na velikom broju poslužitelja elektroničke pošte. Između ostalih korisnici SPF metode su:

- AOL.com
- Altavista.com
- GNU.org
- DynDNS.com
- Earthlink.net
- Google.com
- LiveJournal.com
- MotleyFool.com
- OReilly.com
- Oxford.ac.uk
- PairNIC.com
- Perl.org
- PhilZimmermann.com
- SAP.com
- Symantec.com
- Ticketmaster.com
- w3.org

Poslužitelji elektroničke pošte i *antispam* alati koji podržavaju SPF protokol:

- Sendmail
- Postfix
- Qmail
- Exim
- Microsoft Exchange
- Wildcat
- SpamAssassin
- Sophos
- GFI Software
- Declude Junkmail
- Brightmail
- IronPort
- CipherTrust
- MailArmory
- MailFrontier
- Roaring Penguin Software
- Atlantic Sky
- Communigate Pro

5. Nedostaci SPF protokola

Zbog činjenice da prosljeđivanje poruka elektroničke pošte (eng. *forwarding*) čuva izvornu adresu pošiljatelja, SPF protokol onemogućava klasično prosljeđivanje, uslugu koju pruža velik broj domena poput `pobox.com` odnosno `acm.org`. Ipak, taj je problem riješen SRS (eng. *Sender Rewriting Scheme*) shemom koja korištenjem funkcija sažetka poruke (eng. *hash*) i vremenskih oznaka (eng. *timestamp*) korisnicima omogućava prosljeđivanje poruka. Implementacija SRS-a dostupna je za većinu poslužitelja elektroničke pošte, a moguće ju je nabaviti i u vidu besplatne Perl programske biblioteke `Mail::SRS` dostupne putem CPAN arhive [6].

Drugi veliki nedostatak SPF protokola je tzv. „legitimno lažiranje adrese“. To je situacija kada korisnik posjeduje račun elektroničke pošte na nekom poslužitelju (primjerice `yahoo.com`), ali poštu šalje koristeći SMTP poslužitelj vlastitog pružatelja internetskih usluga (eng. *Internet Service Provider*). Iako zahtjeva određene modifikacije, ovaj je problem rješiv od strane pružatelja internetskih usluga korištenjem „`exists`“ mehanizma.

Pošiljatelj *spam* poruka može zaobići SPF mehanizam registracijom vlastite domene te implementacijom SPF protokola. Ipak, takve je slučajeve moguće osujetiti provjeravanjem *blacklist* popisa baziranih na IP adresama ili nazivima domena. Jedan od mogućih načina rješavanja tog problema je korištenje *greylisting* metode koja neprovjerenim domenama onemogućava trenutnu dostavu poruka elektroničke pošte.

6. Zaključak

Problem *spam* poruka elektroničke pošte potrebno je rješavati na više slojeva. Iako je potpuno onemogućavanje slanja *spam* poruka nemoguće, svaki aspekt *antispam* inicijative postupak slanja čini sve kompleksnijim, a time i ekonomski neisplativim. Veliku efikasnost u blokiranju *spam* poruka SPF protokol pokazao je upravo u kombinaciji s *whitelisting*/*blacklisting* popisima, *greylisting* metodom te neovisnim sustavima akreditacije (npr. *Bonded Sender*, *ISIPP*).
Popularnost SPF protokola između ostalog proizlazi i iz besplatnih nadogradnja za većinu poslužitelja elektroničke pošte koje olakšavaju postupak implementacije SPF protokola, dok je protokol sam po sebi vrlo fleksibilan i nadogradiv (npr. uvođenjem kriptografije) te omogućava postepenu ugradnju.

7. Reference

[1] OpenSPF.org, http://www.openspf.org/
[2] RFC specifikacija SMTP protokola, http://www.faqs.org/rfcs/rfc2821.html
[3] RFC specifikacija SPF protokola, http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-02.txt
[4] Bonded Sender, http://www.bondedsender.com/
[5] Institute for Spam and Internet Public Policy, http://www.isipp.com/
[6] Habeas, http://www.habeas.com/
[7] Mail::SRS http://search.cpan.org/~shevek/
[8] Sender Authentication Deploymeny, http://spf.pobox.com/whitepaper.pdf