Voor- en nadelen van Sender Policy Framework

Ing. K. Trippelvitz & Ing. T. van den Berg

4 februari 2005

Management samenvatting

Het doel van dit project is een onderzoek te doen naar de voor- en nadelen van Sender Policy Framework. SPF heeft als voornaamste doel het tegen gaan van het vervalsen van het envelop From adres in emailberichten. Door een literatuurstudie van verschillende bronnen over SPF is er een analyse gemaakt van de voor- en nadelen van SPF. Op basis hiervan is geconcludeerd dat SPF op dit moment meer en grotere nadelen met zich mee brengt dan voordelen. Hier volgt een opsomming van de grootste voor- en nadelen:

Voordelen:

- Indien er SPF informatie wordt opgenomen in de DNS van een domein kan dit domein niet meer misbruikt worden voor het vervalsen van envelop From headers er van uitgaande dat iedereen SPF controleert.
- In sommige gevallen van SPAM wordt vervalsing van het adres in de envelop From header gebruikt. SPF is bedoeld om dit soort berichten tegen te houden en heeft als voordeel dat het daardoor in zekere zin ook helpt SPAM tegen te houden.

Nadelen:

- SPF maakt gebruik van DNS en omdat DNS problemen omvat met betrekking tot robuustheid, integriteit en betrouwbaarheid is SPF hierdoor niet 100% betrouwbaar.
- De implementatiegraad van SPF is op dit moment nog niet erg hoog in vergelijking tot het aantal in gebruik zijnde domeinen. Dit is een nadeel omdat de effectiviteit van SPF afhangt van de implementatiegraad van SPF.
- Email forwarding waarbij de envelop From header niet herschreven wordt zorgt voor problemen met het gebruik van SPF. Dit heeft als nadeel dat legitieme emailberichten geweigerd kunnen worden. SRS biedt hier een oplossing voor maar deze oplossing heeft als nadeel dat deze alleen werkt als het in elke MTA die forwared geïmplementeerd wordt.

Aan de hand van deze voor- en nadelen wordt aanbevolen om SPF voorlopig nog niet te implementeren. Wellicht kan in de toekomst SPF alsnog geïmplementeerd worden indien deze voor- en nadelen geheel of gedeeltelijk opgelost zijn.

Inhoudsopgave

Hoofdstuk 1

Inleiding

Het doel van dit rapport is het onderzoeken van de voor- en nadelen van SPF. Dit rapport is opgedeeld in een aantal hoofdstukken welke het volgende behandelen:

In het derde hoofdstuk wordt de werking van SPF uitgelegd. Hierbij wordt onder andere gekeken naar de syntax van SPF en worden een aantal voorbeelden gegeven.

Vervolgens wordt in de hoofdstukken vier en vijf geprobeerd om een aantal belangrijke verbanden te leggen met betrekking tot SPF.

Hoofdstuk zeven gaat voornamelijk in op het feit dat SPF gebaseerd is op DNS. Hierbij wordt gekeken naar de mogelijke problemen die dit met zich mee brengt.

De hoofdstukken acht tot en met elf geven een aantal scenario's weer die voorkomen bij normaal gebruik van email. Hier wordt verder ingegaan op de toepassing van SPF op deze scenario's.

Vervolgens wordt er in de hoofdstukken daarna ingegaan op verschillende gerelateerde onderwerpen als MTA's, performance, implementatie en onderhoud.

Tenslotte wordt er een conclusie geformuleerd en wordt er op basis van deze conclusie een aanbeveling gegeven over het wel of niet implementeren van SPF.

Hoofdstuk 2

Project

2.1 Doel van het project

Het doel van dit project is om in opdracht van de subfaculteit Wijsbegeerte een onderzoek te doen naar de voor- en nadelen van Sender Policy Framework (SPF)[3] en om hier een adviesrapport over uit te brengen.

2.2 Projectuitvoering

Het project is uitgevoerd gedurende vier weken en is ingedeeld in drie fases:

1. Oriëntatie
2. Onderzoek
3. Uitloop en adviesrapport schrijven

De eerste fase is uitgevoerd in de eerste week. Gedurende deze week is informatie over SPF verzameld en doorgelezen. Met behulp van deze informatie zijn verschillende onderzoeksvragen opgesteld en aan de hand van deze onderzoeksvragen is een projectvoorstel voor het verloop van het verdere project opgesteld.

De tweede fase van het project is uitgevoerd in de tweede en derde week. Gedurende deze twee weken is geprobeerd om alle opgestelde onderzoeksvragen te beantwoorden.

De laatste week is gebruikt als uitloop voor de onderzoeksfase, het formuleren van de conclusie's, het opstellen van de uiteindelijke aanbeveling en voor het uitschrijven van het adviesrapport.

2.3 Onderzoeksmethodiek

Het onderzoek uitgevoerd voor dit project is een literatuurstudie. Door middel van een document-analyse, dat wil zeggen het raadplegen van verschillende bronnen, is informatie verzameld voor het onderzoek. Op basis van de verzamelde informatie en in samenwerking met de opdrachtgever zijn er verschillende

onderzoeksvragen voor het project gespecificeerd. Door een verdere analyse van de literatuur is geprobeerd de onderzoeksvragen te beantwoorden. Met deze antwoorden is daarna een objectieve conclusie over SPF geformuleerd.

2.4 Terminologie

In dit document wordt gesproken over een deel van een emailbericht bekend onder de volgende termen:

- envelop From header
- envelop From
- return path
- reverse path
- bounce adres
- MAIL FROM

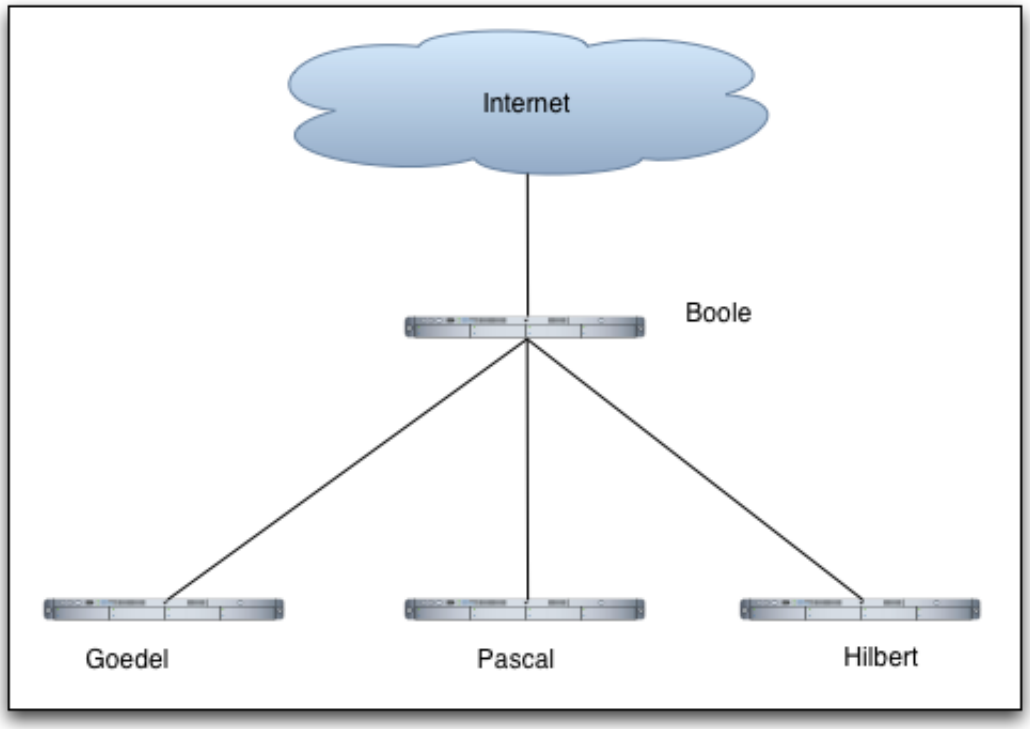
Dit document zal de term "envelop From header" gebruiken. De envelop From header wordt afgeleid van het SMTP MAIL FROM commando. Het adres in de envelop From header is in het algemeen het adres van de afzender en wordt gebruikt om email notificatieberichten heen te sturen.

Als in dit document gesproken wordt over "adresvervalsing" wordt hiermee bedoeld de vervalsing van het adres in de envelop From header.

2.5 Huidige ICT-infrastructuur

Om goed te beoordelen of SPF geschikt is voor de subfaculteit Wijsbegeerte is de email infrastructuur van de subfaculteit Wijsbegeerte in kaart gebracht.

Binnen de subfaculteit Wijsbegeerte wordt gebruik gemaakt van vier SMTP servers. In figuur 2.1 is verder uitgewerkt hoe deze binnen de subfaculteit gebruikt worden.



Figuur 2.1: Email infrastructuur binnen de subfaculteit Wijsbegeerte

Hoofdstuk 3

Werking van SPF

SPF is een protocol dat gebruikt maakt van DNS om het domein van de afzender uit de envelop From header van een email te valideren. SPF maakt gebruik van DNS TXT records of een apart SPF record. In deze velden of records wordt gespecificeerd welke SMTP servers zijn toegestaan om email te versturen voor dat betreffende domein. Elke keer dat er een email wordt ontvangen en SPF is geïmplementeerd wordt er een DNS query gedaan op het domein van het adres in de envelop From header. Het domein van de afzender wordt gehaald uit de from header van de envelop en vervolgens wordt er gekeken naar de geautoriseerde SMTP servers van dat domein. Het IP van de verzendende SMTP server wordt vergeleken met de hosts uit het SPF record van het domein uit de evenlope from header van het emailbericht. Indien de email afkomstig was van een van de geautoriseerde SMTP servers of hosts van het betreffende domein wordt de email toegelaten. Indien de host niet geautoriseerd was om voor dat domein een email te sturen wordt de email bestempeld als een adresvervalsing. In dit geval ligt het aan de instellingen van de SMTP server hoe dit emailbericht wordt afgehandeld. SPF is een protocol dat alleen de identiteit van het verzendende domein garandeerd. SPF heeft geen mogelijkheid om gebruikers te authenticeren. Dat wil zeggen dat SPF geen garantie probeert te geven over welke gebruiker de originele afzender is. SPF probeert alleen garantie te geven tot welk domein de afzender behoort.

3.1 Kanttekening

Voor de correcte werking van SPF moeten aan een aantal voorwaarden kunnen worden voldaan. Ten eerste moet de verzender SMTP servers gespecificeerd hebben die geautoriseerd zijn om voor dat domein email te versturen. Dit gebeurt via SPF entries in de DNS van het domein van de afzender. Ten tweede moet de ontvanger van email om SPF informatie vragen en het ook gebruiken. Als laatste moeten Mail user Agents's(MUA) zo worden geconfigureerd dat het message from adres ook in de envelop From header wordt gezet, oftewel het envelop return adres moet gelijk zijn aan het message from adres. De meeste MUA's doen dit al automatisch, maar in een aantal MUA's kan deze optie worden uitgezet. In dit geval wordt er een return adres gemaakt op basis van de hostname en de gebruikersnaam. Dit kan problemen opleveren met het gebruik

van SPF in bepaalde situaties.

3.2 Syntax

De syntax die gebruikt wordt voor SPF ziet er uit als de normale DNS syntax met daarbij een specifieke syntax voor het textveld van een SPF record. Een DNS entry voor SPF zou er als volgt uit kunnen zien:

```
os3.nl. IN TXT "v=spf1 mx ptr -all"
```

Het “v=” gedeelte geeft de versie van SPF weer die gebruikt word. Er wordt door SPF initieel alleen naar TXT records gekeken waarin het “v=”gedeelte staat. Nadat er een query is gedaan op een TXT record met “v=” informatie worden hieruit de geautoriseerde hosts gehaald.

Deze hosts zijn geautoriseerd om voor dit domein email te versturen. In het geval van het voorbeeld gaat het hier om het MX en PTR record. In plaats van deze twee woorden kunnen ook meerdere MX records of IP ranges genoemd worden. Het ”all” argument matched altijd. In dit geval heeft het een ”-” prefix wat wil zeggen dat elke check die niet op een van de voorgaande argumenten matched een fail krijgt. Er zijn een aantal prefixes die gebruikt kunnen worden, namelijk:

- “-” geeft een fail aan. -all geeft aan dat alles failed en is daarom ook altijd het laatste argument in een SPF record indien het gebruikt word.
- “+” geeft een pass aan. Dit geeft aan dat alle matches een pass krijgen.
- “?” geeft een neutral aan. Dit betekent dat het niet bekend is of het emailbericht is vervalst of niet.
- “∼” geeft een softfail aan. Dit kan gezien worden als een gradatie tussen een fail en een neutral.

3.3 Voorbeelden

In het volgende voorbeeld wordt de werking van SPF nog wat beter toegelicht. Ten behoeve van de voorbeelden wordt aangenomen dat het SPF record er als volgt uit ziet.

```
bron.nl. IN TXT "v=spf1 mx ip4:101.126.56.100 -all"
```

Hiermee wordt aangegeven dat de SMTP servers die geautoriseerd zijn om voor het domein bron.nl email te versturen worden gespecificeerd door het mx record en het IP adres 101.126.56.100. Vervolgens wordt er een email ontvangen bij de SMTP server van het domein doel.nl.

```
HELO bron.nl
250 mail.doel.nl Hello bron.nl [101.126.56.100]
MAIL FROM: afzender@bron.nl
250 afzender@bron.nl... Sender OK
RCPT TO: mlsv@doel.nl
250 mlsv@doel.nl... Recipient OK
```

```
DATA
354 Enter mail, end with "." on a line by itself
From: afzender@bron.nl
To: persoon@doel.nl
.
250 Message accepted for delivery
QUIT
```

SPF zal in dit geval het domein uit de envelop From header halen. Indien de envelop From leeg is gaat SPF er van uit dat de envelop From gecreëerd wordt uit het domein van het EHLO of HELO commando. Vervolgens zal SPF een DNS query doen op het domein bron.nl en hiervan het SPF record evalueren. Uit het SPF record wordt een IP adres gehaald dat wordt vergeleken met het IP adres van de SMTP server die het emailbericht heeft gestuurd (in dit geval is dat 101.126.56.100). Indien 101.126.56.100 overeenkomt met het IP adres uit het SPF record van bron.nl dan wordt de email toegelaten. In dit voorbeeld wordt de email gewoon doorgelaten aangezien hier een match is tussen het IP adres van de SMTP server die de email verzend en het IP adres dat uit het SPF record wordt gehaald van bron.nl, het afzender adres.

In het volgende voorbeeld wordt geïllustreerd hoe een email wordt afgehandeld met een vervalst afzender adres. We nemen in dit geval weer hetzelfde SPF record van bron.nl.

```
HELO bron.nl
250 mail.doel.nl Hello vervalst.nl [101.33.22.181]
MAIL FROM: afzender@bron.nl
250 afzender@bron.nl... Sender OK
RCPT TO: mlsv@doel.nl
250 mlsv@doel.nl... Recipient OK
DATA
354 Enter mail, end with "." on a line by itself
From: afzender@bron.nl
To: persoon@doel.nl
.
250 Message accepted for delivery
QUIT
```

SPF zal in dit geval het domein uit de envelop From header halen. Vervolgens zal SPF een DNS query doen op het domein bron.nl om het SPF record op te halen. Het IP van de verzendende SMTP server, 101.33.22.181, wordt nu vergeleken met het IP in het SPF record van bron.nl, namelijk 101.126.56.100. Hieruit blijkt dat de SMTP server (101.33.22.181) die deze email heeft verstuurd niet geautoriseerd is om email te versturen voor het domein bron.nl. Deze email zal een SPF check niet doorstaan en zal daardoor ofwel gewijgerd worden ofwel bestempeld worden als vervalste email.

Hoofdstuk 4

De binding tussen IP adres en envelop From header

4.1 Onderzoeksvraag

SPF probeert adresvervalsing bij emailberichten tegen te gaan door een verband te leggen tussen het IP adres van de server die het emailbericht verzonden heeft en het domein gebruikt in de envelop From header. Een onderzoeksvraag die hierbij gesteld kan worden is of de binding tussen IP adres/hostname en de envelop From header wel verstandig en goed genoeg is?

4.2 SPF en de opzet van SMTP

SMTP[17] is al vele jaren het protocol dat gebruikt wordt voor het versturen en ontvangen van email. Het doel van SMTP is om betrouwbaar en efficient email te versturen. Een belangrijke eigenschap van SMTP die hiervoor zorgt is "SMTP mail relaying". "SMTP mail relaying" maakt het mogelijk dat emailberichten niet rechtsreeks van de afzender naar ontvanger hoeven te gaan maar ook door tussenliggende machines ontvangen kunnen worden en vervolgens doorgestuurd kunnen worden. Hierdoor is het mogeljk dat een emailbericht vanaf de zender een aantal onbekende en verschillende machines passeert voordat het emailbericht bij de ontvanger terecht komt.

SPF beoogt een verband te leggen tussen het IP adres van de server die het emailbericht verzonden heeft en het domein gebruikt in de envelop From header. Dit concept druist in tegen de zojuist beschreven opzet van SMTP waarbij het mogelijk is dat email via een aantal onbekende machines uiteindelijk bij de ontvanger terecht komt en hierdoor is er in veel gevallen geen verband tussen de verzendende server en het domein gebruikt in de envelop From header. SPF probeert dit verband echter wel te creëren door voor ieder domein te laten vastleggen welke servers geautoriseerd zijn email te versturen in naam van dat domein. Hiermee wordt door SPF in zekere zin geeist dat email rechtstreeks van de zender naar de ontvanger gaat. SPF zorgt dan ook voor problemen bij het doorsturen(forwarden) van email door tussenliggende machines. Deze

problemen worden verder besproken in hoofdstuk twee paragraaf zes.

4.3 IP spoofing

Bij het verband tussen IP adres/hostname en het domein gebruikt in de envelop From header kan er niet vanuit gegaan worden dat de informatie in de envelop From header correct is, daar ligt tenslotte het hele probleem dat SPF oogt op te lossen. Vanwege dit feit moet er automatisch vanuit gegaan worden dat het IP adres van de server die het emailbericht verzonden heeft wel correct is en SPF neemt dit dan ook aan.

Of deze aanname een verstandige aanname is kan in twijfel getrokken worden. Het is namelijk mogelijk voor een kwaadwillig persoon om het IP adres ook te vervalsen, bekend als IP spoofing. Op deze manier kan een kwaadwillig persoon er voor zorgen dat het er op lijkt dat een emailbericht afkomstig is van een geautoriseerde SMTP server voor een domein. SPF zal bij het controleren nu aangeven dat het domein van het adres gebruikt in de envelop From header niet vervalst is, terwijl dit in zo'n geval wel vervalst is.

De bedenkers/ontwikkelaars van SPF lijken het probleem van IP spoofing te erkennen. In twee door verschillende auteurs geschreven Internet-Drafts over SPF[14][15] komt het probleem in het hoofdstuk *Security Considerations* naar voren en wordt het volgende hierover gezegd:

> The client IP address, <IP>, is assumed to be correct. A malicious attacker could spoof TCP sequences to make mail appear to come from a permitted host for a domain that the attacker is impersonating.

Hoewel het probleem in de Internet-Drafts erkend wordt lijkt het probleem in de FAQ op officiële SPF website[3] te worden afgedaan als onbelangrijk. In deze FAQ wordt hier namelijk het volgende over gezegd:

> What about Source IP Spoofing?
>
> Spammers may spoof entire TCP sequences to get their mail out.
>
> Knowledgeable people consider this unlikely. If you think this is a concern, you are invited to demonstrate an attack.

Wie deze zogenoemde *Knowledgeable people* zijn wordt helaas verder niet vermeld. Toch kan het punt dat spammers IP spoofing zouden gebruiken voor het verzenden van grote hoeveelheden spam met vervalste afzender adressen inderdaad als *unlikly* beschouwd worden. Immers wordt er steeds meer gedaan om IP spoofing tegen te gaan waardoor het niet zo makkelijk is om IP spoofing op grote schaal toe te passen. De FAQ spreekt echter niet over een enkel kwaadwillig persoon die maar één bericht wil versturen met gespoofed IP adres. Deze zou hier ondanks dat de kansen steeds kleiner worden nog best wel eens in kunnen slagen, zoals ook vermeld in de Internet-Drafts[14][15].

4.4 Conclusie

Geconcludeerd kan worden dat binding tussen IP adres/hostname en het domein gebruikt in de envelop From header niet betrouwbaar is. Er kan namelijk nooit van uit gegaan worden dat een emailbericht rechtsreeks van de zender naar de ontvanger gaat. SPF bindt domeinen aan een vast aantal machines en omdat SMTP nooit zo opgezet en bedoeld is brengt dit een aantal problemen met zich mee. Er dient echter wel vermeld te worden dat de huidige problemen met adres vervalsing die SPF oogt op te lossen in de tijd dat SMTP werd ontwikkeld niet aanwezig waren. Afhankelijk van hoe erg het probleem van adresvervalsing wordt beschouwd zou hiermee gerechtvaardigd kunnen worden dat SPF in gaat tegen de oorspronkelijke opzet van SMTP en andere problemen oplevert. Op het internet wordt immers al jaren gepraat over het idee om SMTP compleet te vervangen door een verbeterd protocol.

Behalve over de binding zelf kan ook wat gezegd worden over de betrouwbaarheid van de componenten die vergeleken worden. Het gebruik van IP adres als één van deze componenten kan als betrouwbaar beschouwd worden omdat IP spoofing dermate moeilijk is dat het op grote schaal toepassen onmogelijk geacht kan worden. Er moet echter wel altijd in het achterhoofd gehouden worden dat SPF vanwege het IP spoofing probleem niet voor 100% kan garanderen dat het resultaat van een validatie juist is.

Hoofdstuk 5

Adresvervalsing & Spam

5.1 Onderzoeksvraag

Een interessante vraag is of emailberichten met een vals afzender adres op een of andere manier gerelateerd zijn aan spam emailberichten, oftewel het gebruik van adresvervalsing bij het versturen van spam. Mocht er inderdaad een verband zijn dan is het interessant om te kijken of SPF werkelijk invloed kan hebben op het aantal spam emailberichten.

5.2 Identiteit verbergen

Het versturen van spam is in een aantal landen al illegaal en strafbaar. De Verenigde Staten van Amerika heeft in 2003 de CAN-spam act ingevoerd waardoor het versturen van spam strafbaar is geworden. Ook Australia heeft ondertussen een anti-spam wet ingevoerd. Een logische redenatie die hieruit volgt is dat spammers niet graag hun eigen identiteit willen bekend maken. Adresvervalsing kan op deze manier gebruikt worden door spammers om zo de eigen identiteit niet bekend te maken. Een andere reden voor het gebruik van adresvervalsing door spammers is dat het bekend maken van het domein van de spammer waarschijnlijk wordt gevolgd doorhet blacklisten van dit domein. Door adresvervalsing te gebruiken voorkomen spammers dat gauw ontdekt word welk domein wordt gebruikt voor het versturen van spam. Het gevolg hiervan is dat het ook moeilijker is een blacklist bij te houden van domeinen die spam versturen. Ook wordt het moeilijker om te bepalen of domeinen niet per ongeluk op de blacklist gezet zijn door adresvervalsing van spammers. Bijvoorbeeld in het geval dat jouw domein wordt gebruikt door een spammer en het wordt op een blacklist gezet. De eigenaar van het domein is dan niet schuldig aan spammen, maar wel op een blacklist gezet.

5.3 Spam

Een techniek om spam te versturen is het gebruik van adresvervalsing van het return-path van de envelop header en vervolgens het emailbericht te versturen naar een adres dat niet bestaat. Hierdoor kan het emailbericht niet afgele-

verd worden en wordt de email teruggestuurd naar het adres in het return-path van de envelop header. Een spammer kan bijvoorbeeld een email sturen naar blabla261@doel.nl en als return-path opgeven root@blabla.nl. Op deze manier worden alle emailberichten die niet bij het adres blabla261@doel.nl kunnen worden afgeleverd weer terug gestuurd naar root@blabla.nl. Indien blabla261@doel.nl niet bestaat dan worden al deze emailberichten dus teruggestuurd naar root@blabla.nl.

5.4 Spammers

Het zou vreemd genoemd kunnen worden dat veel spammers SPF met open armen hebben ontvangen. De reden hiervoor is dat spammers nu eigen SPF records kunnen specificeren. Hierdoor lijkt spam die afkomstig is van spamdomeinen toch normale email aangezien een SPF check weergeeft dat de SMTP server van de afzender is toegestaan om voor het spamdomein emailberichten te mogen versturen. Spammers kunnen in principe iedereen toestaan om voor hun domein email te versturen. Op deze manier kunnen ze nog steeds zombies gebruiken om spam te versturen en zal een SPF check geen negatief resultaat geven. Het gebruik van zombies om spam te versturen is een van de meest voorkomende manieren om spam te versturen. Dit zal SPF niet tegen houden. Een voorbeeld van een SPF record dat door een spammer gebruik zou kunnen worden is het volgende:

```
spamdomein.com.                IN      TXT     "v=spf1 +all"
```

Het voordeel hiervan is natuurlijk wel dat spammers hierdoor makkelijker te traceren zijn. Op deze manier zullen spammers wel sneller van domeinen moeten verwisselen. Een nuttige vraag die gesteld zou kunnen worden bij dit probleem is in welke mate SPF juist spam doorlaat. Anders gezegd in hoeverre kan SPF juist de oorzaak zijn van het doorlaten van spam. Het antwoord hierop ligt aan de gebruikers van SPF. Het hangt er van af hoe er met SPF informatie omgegaan word en welke andere tests er nog gedaan worden op binnenkomende emailberichten. SPF is niet bedoeld om spam op zichzelf tegen te houden. Het is geen op zichzelf staand anti-spam product. SPF wordt gezien als één test in meerdere die gedaan worden bij het ontvangen van emailberichten en checkt alleen op het gebruik van adresvervalsing. Een SPF check met een PASS als resultaat wil niet zeggen dat het emailbericht geen spam is.

5.5 Conclusie

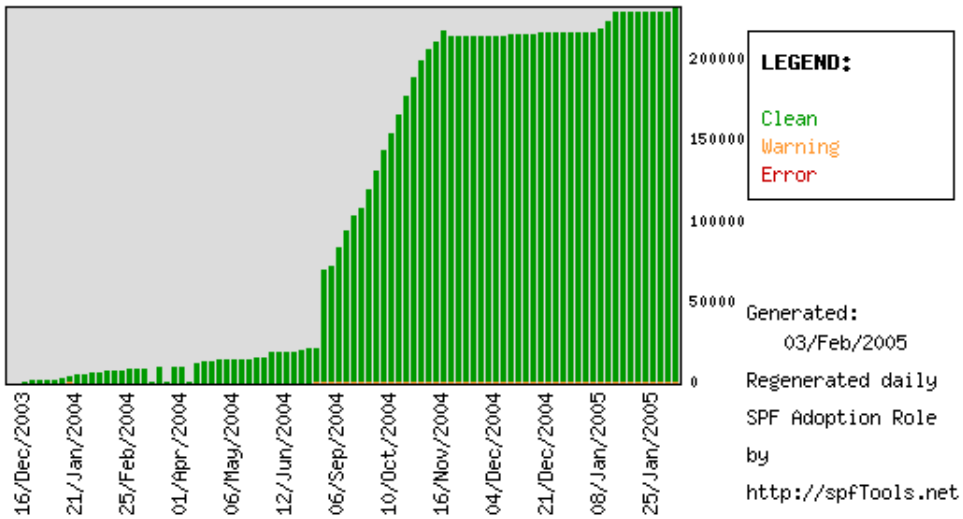
Adresvervalsing wordt wel degelijk gebruikt bij het versturen van spam emailberichten. Hierdoor kan geconcludeerd worden dat SPF een maatregel is wat spam kan tegen gaan. De gebruiker kan zelf instellen hoe er met SPF informatie wordt omgegaan. Er kan bijvoorbeeld voor gekozen worden om alle emailberichten met adresvervalsing direct te weigeren. In dit geval kan er een afname worden waargenomen in het aantal spam emailberichten. Daarentegen is het feit dat het adres van een emailbericht vervalst is geen bewijs dat het een spam emailbericht is. Het zou best zo kunnen zijn dat legitieme emailberichten een vervalst afzender adres hebben.

Hoofdstuk 6

Status en toekomst

6.1 Inleiding

SPF is ontwikkeld met als doel het tegengaan van adresvervalsing. Dit gebeurt door het authenticeren van het domein dat uit de envelop From header gehaald wordt. Op dit moment wordt SPF gebruikt door iets meer dan 200.000 domeinen. Dit lijkt veel maar tegenover het aantal domeinen wat nog steeds geen



Figuur 6.1: Groei van SPF, http://spf.pobox.com/adoption.html

SPF gebruikt is het praktisch niets. Hoewel er nu nog weinig domeinen zijn die het gebruiken is er wel een stijgende lijn aanwezig in het aantal domeinen dat SPF implementeerd. De mate van effectiviteit van SPF hangt uiteraard af van de mate van gebruik. Hoe meer domeinen SPF gaan gebruiken des te effectiever SPF zal zijn.

6.2 Status

Op het moment van schrijven zijn er twee Internet Drafts[14][15] opgesteld met betrekking tot het SPF protocol. Een versie wordt onderhouden door M. Schlitt en de andere versie wordt onderhouden door M. Lentczner. M. Wong, de originele bedenker van SPF werkt ook nog steeds mee aan deze drafts. De nieuwste draft is degene van M. Schlitt en heeft als datum 30 december 2004. De werkgroep, MARID[12], die oorspronkelijk aan de SPF draft werkte bestaat niet meer. Deze groep is eind 2004 uit elkaar gegaan. Het is nu nog onduidelijk wanneer de drafts als officiële standaard zullen worden aangenomen. Op dit moment wordt voornamelijk SPF classic gebruikt. Dit is nog een versie van voor de MARID tijd.

6.3 Toekomst

De toekomstontwikkeling van SPF zou vrij onduidelijk genoemd kunnen worden. Aan de ene kant is er zeker wel een stijging van gebruikers waar te nemen en wordt er verwacht dat deze stijging door zal gaan. Het probleem hierbij is dat het aantal nieuwe domeinen harder groeit dan het aantal domeinen met SPF. Grote domeinen en bedrijven als AOL, Google, w3.org en Symantec hebben SPF al wel geïmplementeerd. Aan de andere kant is de ontwikkeling van het SPF protocol nog vrij onduidelijk. De MARID groep is uit elkaar gevallen en er zijn nu twee verschillende mensen die de SPF drafts onderhouden. Het is nog niet bekend of en wanneer IETF het SPF protocol als officiële standaard zal erkennen. SPF zal alleen nuttig zijn indien het op een grote schaal wordt ingevoerd. Er zijn namelijk twee condities waaraan SPF zal moeten voldoen indien het enigzins succesvol wil zijn. Ten eerste zal SPF compatible moeten zijn met de verschillende MTA's die op dit moment gebruikt worden, oftewel SPF informatie moet wel gebruikt worden. SPF heeft namelijk alleen nut als er ook werkelijk wat met de SPF informatie gedaan wordt. Daarnaast zal SPF op grote schaal ingevoerd moeten worden indien het nuttig wil zijn. Als er maar weinig domeinen zijn die SPF implementeren dan zijn er nog veel domeinen waar nog steeds adresvervalsing vandaan kan komen. Het eigen domein kan in dat geval ook nog steeds vervalst worden indien er bij de ontvanger niet op SPF gecontroleerd wordt.

6.4 Sender-ID & Alternatieven

Microsoft heeft een product ontwikkeld genaamd Sender-ID[13] dat gebruik maakt van SPF. Het kan vergeleken worden met SPF waarbij ook gebruik gemaakt wordt van SRS. Het probleem van Sender-ID is dat het bezwaard is met allerlei patenten. Het is geen open source protocol. Daarnaast zijn er nogal wat kanttekeningen bij het gebruik van Sender-ID. Mede door de patenten en de kanttekening is Sender-ID niet populair. Er is al wel aangekondigd dat Sender-ID geïmplementeerd zal worden in de producten van Microsoft. Op deze manier hoopt Microsoft het gebruik van Sender-ID te vergroten.

Naast Sender-ID zijn er nog verschillende andere alternatieven voor SPF met als belangrijkste variant Domain Keys.

Voor een complete lijst word verwezen naar bijlage B

6.5 Conclusie

De toekomst van SPF is nog onduidelijk. De verantwoordelijke groep mensen bij IETF is uit elkaar gevallen. Daarnaast heeft Microsoft zijn eigen versie op de markt gebracht, namelijk Sender-ID. Aan de andere kant is er wel een stijgende lijn in het gebruik van SPF te zien. Ook is het nog steeds de bedoeling dat SPF een officiële standaard word al is het met enige vertraging. Het is duidelijk dat het succes van SPF afhangt van de mate van gebruik van SPF. Indien SPF niet op grote schaal gebruikt gaat worden is het op zichzelf niet erg nuttig. Voorlopig ziet het er niet naar uit dat SPF in groot gebruik genomen zal worden.

Hoofdstuk 7

Domain Name System

7.1 Onderzoeksvraag

Zoals blijkt uit hoofdstuk twee waarin de werking van SPF wordt uitgelegd is SPF grotendeels gebaseerd op DNS. Bekend en bewezen is echter dat er met DNS een aantal bekende problemen en security issues zijn. Onder andere RFC3833: *Threat Analysis of the Domain Name System (DNS)*[16] beschrijft een groot deel van deze problemen. Wetend dat de opzet van SPF grotendeels op DNS gebaseerd is en dat er bekende problemen met DNS zijn is kan de volgende vraag worden gesteld: Wat voor implicatie heeft de robuustheid, integriteit en betrouwbaarheid van DNS op SPF?

In de volgende paragrafen zullen verschillende problemen met DNS beschreven worden die van invloed kunnen zijn op de werking van SPF.

7.2 DNS onbereikbaar

Het is altijd mogelijk dat de DNS van een domein onbereikbaar is. Dit kan vele verschillende oorzaken hebben waaronder falende harware van de DNS server, falende software, falende netwerkconnectie, etc. Indien DNS voor een domein onbereikbaar is kan het volgende scenario ontstaan:

Een domein bron.nl heeft SPF informatie in zijn DNS opgenomen. Vanwege een onbekende reden is de DNS server voor dit domein tijdelijk niet bereikbaar. De email functionaliteit blijft echter werken. Persoon A van het domein bron.nl stuurt een emailbericht naar persoon B van een ander domein. De SMTP server van dit domein maakt gebruik van SPF om domeinen in afzender adressen te valideren en doet dit dus ook met het emailbericht van persoon A. Voor het valideren wordt de SPF informatie van bron.nl opgevraagd via DNS, dit is nu echter niet mogelijk omdat de DNS server van bron.nl niet bereikbaar is.

Een kwaadwillig persoon zou van dit probleem gebruik kunnen maken door de DNS server van het domein bron.nl aan te vallen en onbruikbaar te maken. Een kwaadwillig persoon is nu in staat om email te sturen uit naam van het domein bron.nl gedurende de tijd dat de DNS server voor dit domein onbereik-

baar is en niemand die deze email ontvangt is in staat te valideren of het domein gebruikt in de envelop From correct is.

Bovenstaand scenario beschrijft hoe afhankelijk SPF is van DNS. Indien de DNS server van een domein onbereikbaar is werkt ook SPF voor dat domein niet meer. Email verstuurd van dit domein kan nu namelijk niet meer gevalideerd worden.

7.3 DNS spoofing

Voor het valideren van het domein in de envelop From header wordt informatie opgehaald uit DNS. Er is echter geen 100% garantie dat het antwoord dat verkregen wordt van de DNS server ook echt door deze DNS server verstuurd is. Een kwaadwillig persoon zou de DNS infrastructuur kunnen aanvallen en ervoor kunnen zorgen dat er gespoofde DNS data terug wordt gezonden. Hiermee heeft dit kwaadwillig persoon direct invloed op de uitslag van de validatie. Het probleem van DNS spoofing wordt onder andere beschreven in RFC3833[16].

Net als met het IP spoofing probleem is ook het DNS spoofing probleem moeilijk op grote schaal toe te passen. Er moet echter net als met het IP spoofing probleem altijd in het achterhoofd gehouden worden dat SPF vanwege het DNS spoofing probleem niet 100% kan garanderen dat het resultaat van een validatie altijd juist is.

7.4 Race conditions

DNS kan gezien worden als een gedistribueerde database, ieder onderhoudt voor zijn eigen domein een DNS. Om te zorgen voor betere performance zijn er servers die DNS resource records van andere DNS server onthouden, ook wel cachen genoemd. Als nu iemand SPF informatie aanpast in zijn DNS kan het enige tijd duren voor de cachende servers ook op de hoogte zijn van deze wijzigingen en beschikken over de nieuwste resource records.

Door bovenstaande beschreven situatie ontstaat een zogenaamde *race condition*. Het volgende scenario kan nu voorkomen:

Een beheerder van domein bron.nl heeft een nieuwe SMTP server in gebruik genomen en voegt deze toe aan de SFP informatie in DNS. Persoon A van bron.nl maakt gelijk gebruik van deze SMTP server door een email te sturen naar persoon B van een ander domein. De SMTP server van dit domein maakt gebruik van SPF om domeinen in afzender adressen te valideren en doet dit dus ook met het emailbericht van persoon A. Voor het valideren wordt de SPF informatie van bron.nl opgevraagd via DNS. De SMTP server vraagt de informatie echter op bij een caching DNS server en krijgt hierdoor een antwoord waarin de wijziging nog niet is verwerkt. Omdat de SMTP server nog niet over de nieuwste informatie beschikt wordt het afzender adres van persoon A's emailbericht nu gezien als vals terwijl deze in dit geval natuurlijk wel correct is.

Door het *race condtion* probleem loopt men de kans dat, indien SPF informatie in DNS gewijzigd wordt, het einige tijd kan duren voor de rest van het internet hier op de hoogte van is. Dit brengt met zich mee dat legitieme emailberichten geweigerd kunnen worden. Om dit probleem te voorkomen dient voorzicht omgegaan te worden met het wijzigen van SPF informatie in DNS en dient tevens goed omgegaan te worden met time-to-die features van DNS.

7.5 TXT record

Voor het publiceren van SPF informatie wordt gebruik gemaakt van een bestaand resource record in DNS, het zogenaamde TXT record[18]. Het TXT record is oorspronkelijk echter niet bedoeld voor het publiceren van SPF informatie en dient voor het publiceren van algemene informatie. Vanwege de volgende feiten maakt SPF toch gebruik van het TXT record:

- SPF beschikt officiëel nog niet over een eigen DNS resource record.
- Er wordt op het internet weinig gebruikt gemaakt van het TXT record voor het publiceren van algemene informatie.

Het kan echter wel voorkomen dat TXT records gebruikt worden voor het publiceren van algemene informatie en indien TXT records te groot worden kan dit voor problemen zorgen. In hoofstuk 3.1.4 van de Internet-Drafts[14][15] wordt de volgende richtlijn gegeven:

> Als de gecombineerde lengte van de DNS naam en alle tekst van alle TXT records beneden de 480 karakters is dan zouden de DNS antwoorden in UDP pakketen moeten passen. Records die te lang zijn om in één enkel UDP pakket te passen zouden kunnen worden genegeerd.

Indien SPF informatie genegeerd wordt heeft dit gevolgen voor het valideren van afzender adressen van emailberichten.

Bovengenoemd probleem zou zich bij een implementatie van SPF alleen voor kunnen doen indien er al gebruikt gemaakt wordt van TXT records in DNS. Zo niet dan heeft het probleem geen invloed op een eventuele implementatie omdat enkel SPF informatie in een TXT record niet boven de 480 karakters zal uitkomen.

7.6 Conclusie

- De bereikbaarheid van een DNS server en dus de betrouwbaarheid van een DNS server kan niet voor 100% gegarandeerd worden en daarmee ook niet de betrouwbaarheid van SPF.
- Door DNS spoofing kan de integriteit van DNS data niet voor 100% gegarandeerd worden en dit heeft direct invloed heeft op de betrouwbaarheid van SPF.

- Door race conditions kan de integriteit van DNS data niet voor 100% gegarandeerd worden en dit heeft direct invloed heeft op de betrouwbaarheid van SPF.
- Door eventuele problemen met te grote TXT records kunnen DNS pakketen genegeerd worden. Dit probleem heeft invloed op de betrouwbaarheid van DNS en daarmee ook op de betrouwbaarheid van SPF.

Mede door de bovenstaande problemen kan geconcludeerd worden dat de robuustheid, integriteit en betrouwbaarheid van DNS een grote implicatie hebben op de goede werking van SPF. De keuze van SPF om gebruik te maken van DNS wordt dan ook als niet verstandig beschouwd en wordt gezien als een minpunt van SPF.

Hoofdstuk 8

Externe Email

Dit hoofdstuk zal alle scenarios behandelen waarbij de afzender van het emailbericht niet per se binnen het netwerk van het domein zit. De scenario's die hier besproken worden zijn de volgende:

- Email versturen vanaf buiten het netwerk van het domein via een andere SMTP server (bijvoorbeeld die van de eigen provider).
- Vanaf buiten het netwerk een tunnel maken naar een computer binnen het netwerk en vanaf deze computer de email versturen gebruik makend van de SMTP server van het netwerk domein.
- Email versturen vanaf buiten het netwerk via de SMTP server van het domein gebruik makend van SMTP authenticatie.

Bij elk scenario wordt een analyse gemaakt hoe SPF in dit geval toegepast kan worden en welke problemen zich voor kunnen doen.

8.1 Externe SMTP server

In dit scenario wordt er gebruik gemaakt van een externe SMTP server om de email te versturen. Dat wil zeggen dat er geen SMTP server wordt gebruikt die afkomstig is van het netwerk van bron.nl, maar in dit geval wordt een SMTP server van xs4all.nl gebruikt. Hierdoor komt de envelop "From" header niet overeen met het afzender adres. Een SPF check op deze email zal in een "FAIL" resulteren.

Voorbeeld:

```
HELO bron.nl
250 mail.doel.nl Hello mail.xs4all.nl [194.109.6.40]
MAIL FROM: kees@bron.nl
250 kees@bron.nl... Sender OK
RCPT TO: mlsv@doel.nl
250 mlsv@doel.nl... Recipient OK
DATA
354 Enter mail, end with "." on a line by itself
```

```
From: kees@bron.nl
To: kees@doel.nl
.
250 Message accepted for delivery
QUIT
```

In dit voorbeeld wordt een email verstuurd van kees@bron.nl naar kees@doel.nl. Beide domeinen hebben SPF geïmplementeerd. De email wordt verstuurd vanaf een thuiswerkplek via de internetprovider die daar voor het internet zorgt. De internetprovider voor deze werkplek is xs4all.nl. De email wordt ook via de SMTP server van xs4all.nl gestuurd, maar uit naam van het domein bron.nl. Het return-path zal dan zijn kees@bron.nl, maar het IP adres van de verzendende SMTP server zal een IP adres zijn uit de range van xs4all.nl. In principe is dit adresvervalsing en SPF zal dit ook interpreteren als adresvervalsing. SPF zal deze email niet doorlaten ondanks dat in dit geval de email wel legitiem is verstuurd uit naam van kees@bron.nl.

Geconcludeerd kan worden dat dit scenario niet meer mogelijk is wanneer SPF geïmplementeerd wordt. De vraag is of dit scenario ook een gewenst scenario is. De functionaliteit die in dit scenario wordt weergegeven zijn op meerdere manieren te bereiken. Een voorbeeld hiervan is precies de werking van het tweede scenario, namelijk een tunnel maken naar het bron.nl netwerk en van daar uit een email versturen.

8.2 Tunnel naar het netwerk

Als oplossing van het vorige scenario zou een tunnel gemaakt kunnen worden naar een computer binnen het bron.nl netwerk. Van daar uit kan dan een email worden verstuurd. In dit geval wordt er wel degelijk een SMTP server gebruikt van het netwerk bron.nl. De afzender of het return-path is ook een adres afkomstig van het bron.nl domein. SPF zal deze email doorlaten ervan uitgaande dat de SMTP server ook werkelijk geautoriseerd is om email te versturen voor het bron.nl.

Voorbeeld:

```
HELO bron.nl
250 mail.doel.nl Hello bron.nl [101.126.56.181]
MAIL FROM: kees@bron.nl
250 kees@bron.nl... Sender OK
RCPT TO: mlsv@doel.nl
250 mlsv@doel.nl... Recipient OK
DATA
354 Enter mail, end with "." on a line by itself
From: kees@bron.nl
To: kees@doel.nl
.
250 Message accepted for delivery
QUIT
```

Vanaf een externe computer (oftewel een computer niet in het netwerk van bron.nl) wordt een tunnel gemaakt naar een computer binnen het netwerk van bron.nl. Hierbij wordt gebruik gemaakt van SSH. Wanneer de tunnel tot stand is gekomen wordt er een email verstuurd naar kees@doel.nl vanaf de computer in het netwerk van bron.nl. Het return-path van de afzender is in dit geval kees@bron.nl. Deze email wordt opgepakt door de SMTP server van het bron.nl domein en verstuurd het emailbericht. In dit geval is de versturende SMTP server geautoriseerd om voor bron.nl email te versturen. Bij ontvangst in het doel.nl domein wordt er een DNS query gedaan op het SPF record van bron.nl. Hierin staat het IP van de geautoriseerde SMTP server (in dit geval ook de verzendende email server). Dit IP adres wordt vergeleken met het IP adres van de verzendende SMTP server. In dit geval komen ze overeen en wordt het emailbericht doorgelaten.

In dit geval is er in principe geen probleem te onderkennen. Het IP waarvan de email vandaan komt is geautoriseerd om voor dit domein email te versturen.

8.3 SMTP Authenticatie

Een andere mogelijkheid om email te versturen vanaf bijvoorbeeld een thuiswerkplek is SMTP authenticatie. Hierbij wordt SMTP authenticatie gebruikt om een verbinding tot stand te brengen direct met een SMTP server en die het emailbericht te laten versturen.

Voorbeeld:

```
EHLO bron.nl
250 mail.doel.nl Hello bron.nl [101.126.56.181]
AUTH LOGIN
334 VXNlcm5hbWU6
a4msl9ux
334 UGFzc3dvcmQ6
ZvVx9G1hcg==
235 2.0.0 OK Authenticated
MAIL FROM: kees@bron.nl
250 kees@bron.nl... Sender ok
RCPT TO: mlsv@doel.nl
250 mlsv.@doel.nl... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: kees@bron.nl
To: kees@doel.nl
.
250 Message accepted for delivery
QUIT
```

Vanaf een externe computer wordt, met behulp van SMTP authenticatie, een connectie gemaakt met de SMTP server van het bron.nl netwerk. Vervolgens wordt er een emailbericht verstuurd vanaf de externe computer via de SMTP server van het bron.nl netwerk. In dit geval ziet de envelop van het emailbericht

er vrijwel hetzelfde uit als bij het vorige scenario. Er is voor de werking van SPF in ieder geval geen verschil. Op deze manier kan er ook vanaf externe computers email verstuurd worden.

8.4 Webmail

In dit scenario wordt gebruik gemaakt van een webmail service. Hierbij wordt gebruik gemaakt van een webinterface om bijvoorbeeld de email van de eigen werkplek te beheren. In de meeste gevallen wordt hier de SMTP server gebruikt van het netwerk waar de webmail service draait.

Voorbeeld: Er wordt vanaf een thuiswerkplek ingelogd op de webmail service van het bron.nl domein. Hier vandaan verstuurd piet een email naar paul@doel.nl. De webmail service verstuurd de email via de SMTP server van het bron.nl domein. Op deze manier kan vanaf welke locatie dan ook legitieme mail verstuurd worden uit naam van het bron.nl domein. Het afzender adres in de envelop From header is in dit geval piet@bron.nl. Een SPF controle aan de kant van het doel.nl domein zal in dit geval een PASS opleveren.

Het gebruik van webmail zorgt ervoor dat er vanaf welke locatie dan ook legitieme email verstuurd kan worden. Webmail is in dit geval zeker een goede oplossing voor het van afstand versturen van email. SPF zal in met dit scenario zeker geen problemen geven.

8.5 Conclusie

De voorgaande voorbeelden of scenario's geven een aantal situaties weer die niet ondenkelijk zijn in het dagelijks gebruik van email. Deze scenario's geven weer dat zoiets als bijvoorbeeld thuiswerken met SPF nog steeds mogelijk is. Het enige nadeel is dat het aantal manieren waarop dit kan gebeuren minder wordt door het gebruik van SPF. Natuurlijk zijn er altijd variaties en andere scenario's waarin SPF een probleem vormt voor de correcte werking van email.

Hoofdstuk 9

Interne email

Dit hoofdstuk zal behandelen waarbij de afzender van het emailbericht binnen het netwerk van het domein zit. Tevens zal gekeken worden hoe SPF omgaat met binnenkomende emailberichten die intern geforward worden.

9.1 Uitgaande email

SPF gaat er voornamelijk vanuit dat email communicatie bestaat uit een transactie tussen zogenaamde border SMTP servers van verschillende netwerken. Deze zogenaamde border SMTP servers dienen gespecificeerd te worden in het SPF record. In figuur 2.1 zou dit de server “Boole” zijn. Voor de goede werking van SPF maakt het niet uit hoe vaak een emailbericht door interne SMTP servers geforward wordt, zolang het emailbericht uiteindelijk via een geautoriseerde SMTP server het netwerk verlaat.

9.2 Binnenkomende email

SPF gaat er voornamelijk vanuit dat email communicatie bestaat uit een transactie tussen zogenaamde border SMTP servers van verschillende netwerken. De meest toegepaste methode is om binnenkomende emailberichten te controleren bij binnenkomst van het netwerk oftewel de border SMTP server. Voor de goede werking van SPF maakt het niet uit hoe een emailbericht vervolgens intern geforward en bij de ontvanger afgeleverd wordt.

9.3 Conclusie

Uit de voorgaande paragrafen blijkt dat SPF voor zover er is geconstateerd geen problemen oplevert met de scenario’s die in deze paragrafen beschreven zijn.

Hoofdstuk 10

Email forwarden

In hoofdstuk 2 paragraaf 2.2 is naar voren gekomen dat er schijnbaar problemen zijn tussen de werking van SPF en het forwarden van email. In dit hoofdstuk wordt naar verschillende manieren van email forwarding gekeken en wat de werking van SPF is in elk geval.

10.1 Aliases

In RFC1123[19] wordt het begrip *alias* als volgt gedefinieerd:

> To expand an alias, the recipient mailer simply replaces the pseudo-mailbox address in the envelope with each of the expanded addresses in turn; the rest of the envelope and the message body are left unchanged. The message is then delivered or forwarded to each expanded address.

Het bovenstaande beschreven concept van aliases is een veel gebruikt concept, enkele voorbeelden zijn:

- Gebruikers die bijvoorbeeld via .forward files hun emailberichten van een mailbox forwarden naar een andere mailbox.
- Bedrijven met alias mailboxes zoals administatie@bron.nl waarbij een emailbericht naar dit adres wordt doorgestuurd naar alle administratiemedewerkers.
- /etc/aliases in Sendmail.

Uit de beschrijving van het begip alias zoals gegeven in RFC1123 blijkt dat bij het doorsturen(forwarden) van emailberichten het adres in de envelop From header niet veranderd wordt. Hierdoor ontstaat een probleem waardoor de werking van SPF en het gebruik van aliases niet goed samen gaan. In het volgende scenario zal dit duidelijk gemaakt worden:

Het domein bron.nl heeft SPF informatie opgenomen in DNS. Persoon A van het domein bron.nl stuurt een emailbericht naar persoon B van domein forward.nl. Dit emailbericht wordt ontvangen door de SMTP server van forward.nl. Deze stuurt het emailbericht door naar een adres van persoon B bij domein doel.nl.

De SMTP server van domein doel.nl maakt gebruik van SPF voor validatie. Dit valideren zal nu echter niet goed gaan. Het emailbericht van persoon A van domein bron.nl wordt namelijk als laatste verstuurd via de SMTP server van domein forward.nl en het IP adres van deze server wordt gebruikt voor validatie. Het envelop From adres verwijst nog steeds naar domein bron.nl. In het SPF record van bron.nl zal het IP adres van de SMTP server van doel.nl echter niet voorkomen. Hierdoor lijkt de envelop From vervalst en zal het emailbericht geweigerd worden.

Hieronder staat het scenario nog in het kort weergegeven:

Hop	Client ID	Ontvanger	envelop From	SPF check
1	bron.nl	persoon-b@forward.nl	persoon-a@bron.nl	Accept
2	forward.nl	persoon-b@doel.nl	persoon-a@bron.nl	Reject

Om SPF wel te laten werken had de SMTP server van forward.nl de envelop From moeten veranderen in een adres dat eindigd op forward.nl. Hieronder wordt een voobeeld gegeven waarbij het adres wel herschreven wordt en waarbij SPF wel werkt:

Hop	Client ID	Ontvanger	envelop From	SPF check
1	bron.nl	persoon-b@forward.nl	persoon-a@bron.nl	Accept
2	forward.nl	persoon-b@doel.nl	persoon-b@forward.nl	Accept

Hoewel SPF het emailbericht nu zal accepteren brengt het op deze manier van herschrijven van de envelop From een ander probleem met zich mee. Indien het emailbericht in dit geval namelijk bounced komt deze melding terecht bij de forwarder in plaats van de orginele zender. Om dit goed te laten verlopen is een oplossing aanwezig in de vorm van SRS(zie 10.4).

10.2 Fallback MX

Eén van de aspecten van de opzet van SMTP is het gebruik van fallback mail exchangers(MX). Dit houdt in dat als de primary MX van een domein niet meer in staat is email te ontvangen een andere server(fallback MX) deze taak kan overnemen. Deze houdt de email nu net zo lang vast tot dat de primary MX weer “up” is en stuurt dan alle verzamelde email door naar de primary MX.

De werking van fallback MX gaat niet goed samen met SPF. Dit om de zelfde reden als beschreven in paragraaf 10.1. Ook bij het vasthouden en doorsturen van de email wordt het adres in de envelop From header niet herschreven. Dit probleem leidt tot de conclusie dat indien SPF gebruikt wordt op de primary MX het gebruik van een fallback MX onmogelijk wordt indien deze de envelop From niet herschrijft.

10.3 Mailinglijsten

In RFC1123[19] wordt het begrip *list* als volgt gedefinieerd:

> A mailing list may be said to operate by "redistribution" rather than by "forwarding". To expand a list, the recipient mailer replaces the pseudo-mailbox address in the envelope with each of the expanded addresses in turn. The return address in the envelope is changed so that all error messages generated by the final deliveries will be returned to a list administrator, not to the message originator, who generally has no control over the contents of the list and will typically find error messages annoying.

Uit de beschrijving van RFC1123 blijkt dat bij het forwarden van emailberichten het adres in de envelop From header wel veranderd wordt. Hierdoor hebben de werking van SPF en de werking van mailinglijsten geen invloed op elkaar. Emailberichten verstuurd naar en door maillijsten zullen een SPF validatie goed doorstaan.

10.4 Sender Rewriting Scheme

Zoals is gebleken uit de paragrafen 10.1 en 10.2 ontstaan er problemen met SPF en het forwarden van email indien het adres in de envelop From header niet herschreven wordt. Het was ook bekend dat om dit probleem op te lossen dient de envelop From herschreven te worden maar hierdoor ontstaat weer een nieuw probleem ontstaat.

Op de officiële website van SPF[3] wordt erkend dat SPF problemen heeft met email forwarding. Hiervoor wordt een oplossing geboden in de vorm van het "Sender Rewriting Scheme" afgekort als "SRS"[5]. SRS zorgt er in het kort gezegd voor het herschrijven van de envelop From en houdt ook rekening met het bouncen van email. In figuur 10.1 is te zien hoe SRS de envelop From herschrijft.

Figuur 10.1: Werking SRS, http://spf.pobox.com/srspng.html

De herschreven envelop From in het figuur kan opgedeeld worden in meerdere delen:

SRS0: Dit verteld aan andere forwarders dat SRS al een keer is uitgevoerd. Een volgende forwarder met SRS maakt nu van SRS0 SRS1. Bij nog een extra forward wordt het getal niet meer verhoogd.

yf09: Dit is een voorbeeld van een hash. De hash dient er voor om te zorgen dat forwarders niet als open relay gebruikt kunnen worden.

Cw: Dit is een voorbeeld van een timestamp. Deze dient om de geldigheid van het door SRS gecreeerde email adres te laten verlopen.

orig.com=ann: Mocht cob@third.com onbereikbaar zijn dan krijgt pobox.com een bounce. Door het *orig.com=ann* gedeelte weet deze nu wat de origenele afzender was en stuurt de bounce door naar dit adres.

@pobox.com: Dit is het gedeelte dat er voor zorgt dat het emailbericht door de test van SPF komt.

Hoewel SRS de ideale oplossing lijkt voor het oplossen van het forward probleem zijn er nog wel enkele kanttekeningen. Onder andere Jonathan de Boyne Pollard behandeld in zijn artikel[10] over SPF deze kanttekeningen.

10.5 Conclusie

Geconcludeerd kan worden dat SPF en email forwarding op slechte fout met elkaar staan. Volgens de SMTP specificatie[17] hoeft bij het forwarden van email het adres in de envelop From niet herschreven te worden en voor de goede werking van SPF wordt geëist dat dit wel gebeurd. Om dit herschrijven goed te laten verlopen is SRS ontwikkeld. Er is echter één probleem:
Mensen die SPF steunen en implementeren zullen ook SRS gaan gebruiken indien zij email forwarden. Het probleem is dat een groot deel van de internet community nog geen gebruik maakt van SPF en deze zien er niets in om SRS op hun MTA te implementeren. Zolang niet elke MTA gebruik maakt van SRS of een andere manier van herschrijven ontstaan twee problemen die een ernstig nadeel vormen van SPF:

1. Probleem bij de ontvangende kant: Indien een ontvangende SMTP server geconfigureerd met SPF een emailbericht ontvangt van een domein dat SPF gebruikt en dat onderweg een keer is geforward door een SMTP server zonder SRS zal dit bericht niet door de SPF validatie komen. Omdat SRS nog niet op grote schaal is toegepast ontstaat hier door de kans dat grote aantallen emailberichten geweigerd worden die wel legitiem zijn.

2. Probleem bij de verzendende kant: Het probleem voor de verzendende kant is in feite het zelfde als het bovenstaande probleem. Indien SPF geconfigureerd wordt in DNS ontstaat de kans dat verzonden emailberichten die onderweg geforward worden, geweigerd worden door de ontvanger.

De vraag is dan ook of SPF nog steeds gebruikt moet worden indien SRS niet algemeen geaccepteerd en gebruikt wordt.

Hoofdstuk 11

Meerdere domeinen

Bij het beheren van meerdere domeinen zou er een probleem kunnen ontstaan bij het gebruik van SPF wanneer er maar één SMTP server gebruikt wordt om voor alle domeinen email te versturen. In dat geval is één SMTP server geautoriseerd om voor meerdere domeinen email te versturen. Hierdoor zouden gebruikers van het ene domein zich voor kunnen doen als gebruikers van het andere domein.

Voorbeeld: In dit voorbeeld worden twee domeinen beheerd, namelijk bronA.nl en bronB.nl. Een gebruiker van het bronA.nl netwerk wil een vervalste email sturen naar doel.nl. In dit geval kan de gebruiker van bronA.nl een email sturen uit naam van een gebruiker van bronB.nl. SPF kan op geen enkele wijze ontdekken of de email authentiek is of dat hij vervalst is aangezien beide domeinen dezelfde SMTP server gebruiken. Voor beide domeinen staat in het SPF record dezelfde SMTP server.

Hieruit kan geconcludeerd worden dat SPF geen garanties geeft tegen adresvervalsing geeft. Bij het gebruik van meerdere domeinen en één SMTP server kan nog steeds adresvervalsing voorkomen.

Hoofdstuk 12

MTA's en anti-spam producten

12.1 Onderzoeksvraag

SPF is geen op zich zelf staand stuk software maar dient geintergreerd te worden in Mail Transfer Agent software of een anti-spam product. Binnen de subfaculteit Wijsbegeerte wordt Postfix[1] gebruikt als MTA en SpamAssassin[2] als anti-spam product. Een voorwaarde voor de implementatie van SPF is dat SPF met deze beide of één van deze producten te gebruiken is. De vraag wordt daarom gesteld hoe de ondersteuning van MTA's en anti-spam producten is voor SPF met daarbij in het bijzonder de ondersteuning van Postfix en SpamAssasin.

12.2 MTA's

Op de markt zijn vele soorten MTA's te verkrijgen. Van commerciële tot open source producten en van simpele tot hele uitgebreide producten. Gebleken is dat nog niet alle MTA's beschikken over mogelijkheden om gebruik te maken van SPF. Hierbij zijn het vooral de kleinere en/of commerciële MTA producten die nog niet beschikken over deze mogelijkheid. Indien het hier gaat over een open source MTA is er nog wel de mogelijkheid om deze functie zelf te ontwikkelen. Er zijn in verschillende programmeertalen geschreven libraries beschikbaar die hiervoor gebruikt kunnen worden.[4]

Voor de volgende MTA's zijn wel verschillende soorten patches/modules aanwezig om SPF mogelijk te maken:

- Postfix
- Sendmail
- Qmail
- Exim
- Courier

- MS Exchange
- OmniTI Ecelerity

Hierbij moet wel vermeld worden dat nog niet al deze patches/modules geoptimaliseerd zijn en correct werken. Dit komt mede door het feit dat deze patches en modules in de meeste gevallen ontwikkeld worden door verschillende derde partijen en niet door de ontwikkelaars van de MTA zelf.

12.3 Anti-spam producten

Het is ondoenlijk gebleken om te onderzoeken hoe het staat met de ondersteuning van anti-spam producten voor SPF, hiervoor is het aantal beschikbare anti-spam producten te groot. Vanwege deze reden is alleen gekeken naar SpamAssassin, het anti-spam product gebruikt binnen de subfaculteit Wijsbegeerte.

SPF wordt door SpamAssassin ondersteund vanaf versie 3.0 doormiddel van een bijgeleverde plugin. Deze plugin kan gebruikt worden door in het configuratiebestand van SpamAssassin de volgende regel toe te voegen: loadplugin Mail::SpamAssassin::Plugin::SPF . Om gebruik te maken van deze plugin dienen wel de volgende twee perl modules geïstalleerd te zijn:

- Mail::SPF::Query[3][9]
- Net::DNS[9]

Getest kan worden of deze modules geinstalleerd zijn door in de shell het volgende uit te voeren: perl -e 'require *modulenaam*' . Indien de volgende error "Can't locate Mail/SPF/Query.pm in @INC..." of een soortgelijke error verschijnt is een module nog niet aanwezig. Deze kan vervolgens gedownload worden van CPAN[9].

SpamAssassin bepaald of een emailbericht SPAM is aan de hand van de uitkomsten van een set van regels/tests. Indien de SPF module geladen is wordt er een regel toegevoegd welke het verband onderzoekt tussen het IP adres van de verzendende server en het domein in de envelop From. Afhankelijk van de uitkomst komt hier een bepaalde score uit die van invloed is om vast te stellen of een emailbericht SPAM is.

12.4 Conclusie

Geconcludeerd kan worden dat de ondersteuning van alle bekende MTA's voor SPF goed is. Ook de door de subfaculteit Wijsbegeerte gebruikte producten Postfix en SpamAssassin werken goed samen met SPF. Een nadeel is wel dat de ondersteuning vaak afhankelijk is van derde partijen en dat toch nog een redelijk aantal MTA's geen ondersteuning heeft voor SPF. Om SPF te laten slagen zou als voorwaarde gesteld kunnen worden dat alle MTA standaard out-the-box SPF ondersteunen.

Hoofdstuk 13

Performance

13.1 Onderzoeksvraag

Bij het gebruik van SPF wordt van elk binnenkomend emailbericht het domein in de envelop From vergeleken met het IP adres van de verzendende server. Dit zou kunnen zorgen voor een zekere belasting van het systeem die deze controle moet uitvoeren. De vraag is in dit geval in hoeverre het gebruik van SPF de performance van een systeem en netwerk beïnvloed. Dit kan een belangrijke kwestie zijn indien er bijvoorbeeld nog steeds per mb voor bandbreedte betaald wordt of als er gebruik gemaakt wordt van oudere hardware.

13.2 Overhead

De belangrijkste overhead die SPF veroorzaakt voor een systeem en netwerk is het uitvoeren van DNS queries. Voor elk emailbericht dat binnenkomt moet minimaal één DNS query worden gedaan om de SPF informatie op te halen. Hierna zullen bijna altijd nog extra queries uitgevoerd moeten worden om A, MX of PTR records op te vragen. Hypothetisch wordt er nu vanuit gegaan dat gemiddeld drie queries per SPF controle nodig zijn. Evenredig met het aantal emailberichten dat binnenkomt zullen het aantal uit te voeren DNS queries met een factor drie stijgen. DNS werkt met UDP en is een relatief goedkoop protocol qua bandbreedte en benodigde CPU kracht. Hierdoor zou de overhead van de extra queries beperkt moeten blijven.

Om percentages over de overhead te verkrijgen zullen tests uitgevoerd moeten worden. Een manier om de overhead te testen zou kunnen zijn door het opzetten van twee SMTP servers met de zelfde hardware waarvan één geconfigureerd met SPF en één zonder SPF. Nu dient naar beide machines een vast aantal emailberichten gestuurd te worden en performance vergeleken te worden. Deze expirimenten zijn vanwege tijdsgebrek buiten de beschouwing van dit project gelaten.

13.3 DDOS

Een interessante vraag die op het gebied van performance gesteld kan worden is in hoeverre SPF gebruikt kan worden voor het doen van zogenaamde "distributed Denial Of Service" aanvallen. Een aanvaller zou een gedistribueerde aanval kunnen uitvoeren door vanaf vele clients(zombies) veel emailberichten te versturen met als envelop From adres bron.nl. Indien er op al deze emailberichten een SPF check wordt gedaan betekent dit dat er voor elk emailbericht een DNS query wordt gedaan op de DNS server van bron.nl. Als er maar genoeg emailberichten gecontroleerd dan zou dit hypothetisch kunnen resulteren in een DOS van de DNS server van bron.nl.

13.4 Conclusie

Hoewel het gebruik van SPF relatief veel extra DNS queries met zich mee brengt wordt verondersteld dat de overhead hiervan qua bandbreedte en CPU kracht verwaarloosbaar is. Ondanks dat dit niet getest is kan veilig geconcludeerd worden dat de performance kwestie geen beslissende factor is bij het oordeel over het gebruik van SPF.

Hoofdstuk 14

Implementatie en onderhoud

14.1 Onderzoeksvraag

Veel software of nieuwe technieken zijn moeilijk te implementeren in een bestaande organisatie. Ook het onderhouden van een systeem is vaak problematisch, mede omdat ICT organisaties snel kunnen veranderen. De vraag die gesteld wordt is dan ook hoe moeilijk het is om SPF te implementeren en te onderhouden.

14.2 Implementatie

Bij de implementatie van SPF zijn er een aantal punten die van belang zijn:

- Er moet beslist worden welke SMTP servers geautoriseerd zijn om voor het domein email te versturen. Dit hangt natuurlijk af van de structuur van het netwerk. Vooral in wat grotere organisaties kan dit wat werk met zich meebrengen

- De SPF records dienen gespecificeerd en in DNS toegevoegd te worden. Afhankelijk van de grote van een organisaties wordt het specificeren van het SPF record meer complex. Voor kleinere organisaties kan gebruikt gemaakt worden van een "wizard" op de SPF homepage[3]. Voor grotere organisaties wordt aangeraden de Internet Drafts goed te bekijken om de syntax van het SPF record goed te leren begrijpen en zo zelf het record op te stellen.

- Om inkomende emailberichten te controleren op SPF dient SPF geïmplementeerd te worden in één of meerdere MTA's. Hiervoor dient in het algemeen een patch/of module toegevoegd te worden aan de MTA.

  Er dient wel goed bepaald te worden op welke SMTP servers SPF wordt geïmplementeerd om te controleren. In de Internet Drafts over SPF[14][15] wordt aangeraden dit te doen op de SMTP servers die aan de grenzen van

het netwerk staan.

- Indien er binnen het netwerk ook aan mailforwarding wordt gedaan is het nuttig om ook SRS te implementeren en onderhouden op de plaatsen waar email wordt geforward. Dit houdt in dat op de MTA's die forwarden een SRS patch of module toegevoegd moet worden.

14.3 Onderhoud

Het onderhouden van SPF bestaat in principe uit twee taken:

- Het bijhouden van het SPF record. Dit zal alleen moeten gebeuren in het geval er een SMTP sever verdwijnt, een SMTP server bijkomt of SMTP servers een ander IP adres krijgen. Ervan uitgaand dat deze gevallen niet al te vaak voorkomen zal het onderhoud aan het SPF record erg beperkt zijn
- Het up-to-date houden van de SPF patches/modules voor de MTA software. Over het algemeen zullen, indien SPF eenmaal geïmplementeerd is op in een MTA, geen veranderingen meer hoeven worden aangebracht. Wel dient er goed opgelet te worden of patches/modules nog werken als er een nieuwere versie van de MTA wordt geïnstalleerd of als wordt overgeschakeld naar een ander soort MTA.

14.4 Conclusie

Geconcludeerd kan worden het het implementeren van SPF nog redelijk wat stappen vereist. De belangrijkste stap is het nadenken over welke SMTP servers gespecificeerd worden en op welke servers gecontroleerd wordt op SPF. De rest van de stappen brengen relatief weinig werk met zich mee.

Het onderhoud van SPF is minimaal. Alleen bij veranderingen van de email infrastructuur binnen een organisatie zal dit gevolgen hebben voor SPF.

Hoofdstuk 15

Conclusie & aanbevelingen

In dit hoofdstuk zullen alle voor- en nadelen van SPF nog een keer op een rij worden gezet. Aan de hand van deze korte samenvatting wordt dan een conclusie gevormd met betrekking tot SPF. Afhankelijk van deze conclusie wordt een aanbeveling gedaan aan de subfaculteit Wijsbegeerte over het gebruik van SPF.

15.1 Voordelen

1. Indien er SPF informatie wordt opgenomen in de DNS van een domein kan dit domein niet meer misbruikt worden voor het vervalsen van envelop From headers er van uitgaande dat iedereen SPF controleert.
2. In sommige gevallen van SPAM wordt vervalsing van het adres in de envelop From header gebruikt. SPF is bedoeld om dit soort berichten tegen te houden en heeft als voordeel dat het daardoor in zekere zin ook helpt SPAM tegen te houden.
3. SPF is relatief simpel te implementeren en te onderhouden.
4. SPF is niet bezwaard met patenten en licenties.
5. Voor alle bekende MTA's zijn patches/modules beschikbaar om gebruik te kunnen maken van SPF.

15.2 Nadelen

1. SPF maakt gebruik van DNS en omdat DNS problemen omvat met betrekking tot robuustheid, integriteit en betrouwbaarheid is SPF hierdoor niet 100% betrouwbaar.
2. SPF is op dit moment nog geen officiële standaard. Dit zou mensen er van kunnen weerhouden om SPF te gebruiken.
3. De implementatiegraad van SPF is op dit moment nog niet erg hoog in vergelijking tot het aantal in gebruik zijnde domeinen. Dit is een nadeel omdat de effectiviteit van SPF afhangt van de implementatiegraad van SPF.

4. De ondersteuning van SPF voor MTA's hangt voorlopig af van patches/modules gemaakt door derde partijen.

5. Er gaat email functionaliteit verloren doordat SPF het gebruik van SMTP servers limiteert.

6. Email forwarding waarbij de envelop From header niet herschreven wordt zorgt voor problemen met het gebruik van SPF. Dit heeft als nadeel dat legitieme emailberichten geweigerd kunnen worden. SRS biedt hier een oplossing voor maar deze oplossing heeft als nadeel dat deze alleen werkt als het in elke MTA die forwared geïmplementeerd wordt.

7. Bij het gebruik van meerdere domeinen in samenwerking met één SMTP server is het niet mogelijk om vervalsing van de envelop From header compleet tegen te gaan. Gebruikers van het ene domein kunnen zich voor doen als gebruikers van het andere domein.

15.3 Conclusie

Hoewel het doel en zowel het grootste voordeel van SPF, het tegen gaan van envelop From vervalsing, een nobel streven is weegt dit niet op tegen enkele ernstige nadelen. Deze nadelen omvatten voornamelijk de problematiek rond forwarden, zoals de kans dat legitieme emailberichten geweigerd kunnen worden, en de problematiek met DNS.

15.4 Aanbevelingen

Op basis van de genoemde voor- en nadelen wordt aangeraden aan om SPF voorlopig niet te implementeren binnen de subfaculteit Wijsbegeerte. Indien SPF en SRS in de toekomst algemeen geaccepteerde standaarden worden wordt aangeraden de voor- en nadelen opnieuw tegen elkaar af te wegen.

Als advies wordt gegeven dat naar eventuele alternatieven van SPF met soort gelijke mogelijkheden gekeken kan worden. Dit is binnen dit project buiten beschouwing gelaten. Voor een complete lijst met alternatieven word verwezen naar bijlage B

Bibliografie

[1] Postfix homepage, http://www.postfix.org

[2] SpamAssassin homepage, http://spamassassin.apache.org

[3] SPF homepage, http://spf.pobox.com

[4] SPF libraries, patches, modules, http://spf.pobox.com

[5] SPF homepage about SRS, http://spf.pobox.com/srs.html

[6] Wikipedia, http://en.wikipedia.org/wiki/Sender_Policy_Framework

[7] AOL SPF informatie, http://postmaster.aol.com/info/spf.html

[8] http://wiki.mutt.org/index.cgi?MuttFaq/Header

[9] Comprehensive Perl Archive Network, http://www.cpan.org

[10] http://homepages.tesco.net/∼J.deBoynePollard/FGA/smtp-spf-is-harmful.html

[11] http://www.stopspam.org/email/headers.html

[12] http://www.ietf.org/html.charters/OLD/marid-charter.html

[13] Sender-ID Framework, http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx

[14] W. Schlitt & M. Wong, *Sender Policy Framework: Authorizing Use of Domains in E-MAIL*
www.ietf.org/internet-drafts/draft-schlitt-spf-classic-00.txt
30 december 2004

[15] M. Lentczner & M. Wong, *Sender Policy Framework: Authorizing Use of Domains in MAIL FROM*
www.ietf.org/internet-drafts/draft-lentczner-spf-00.txt
12 oktober 2004

[16] D. Atkins & R. Austein, *Threat Analysis of the Domain Name System (DNS)*
http://www.ietf.org/rfc/rfc3833.txt
augustus 2004

[17] J. Klensin, *Simple Mail Transfer Protocol*
http://www.ietf.org/rfc/rfc2821.txt april 2001

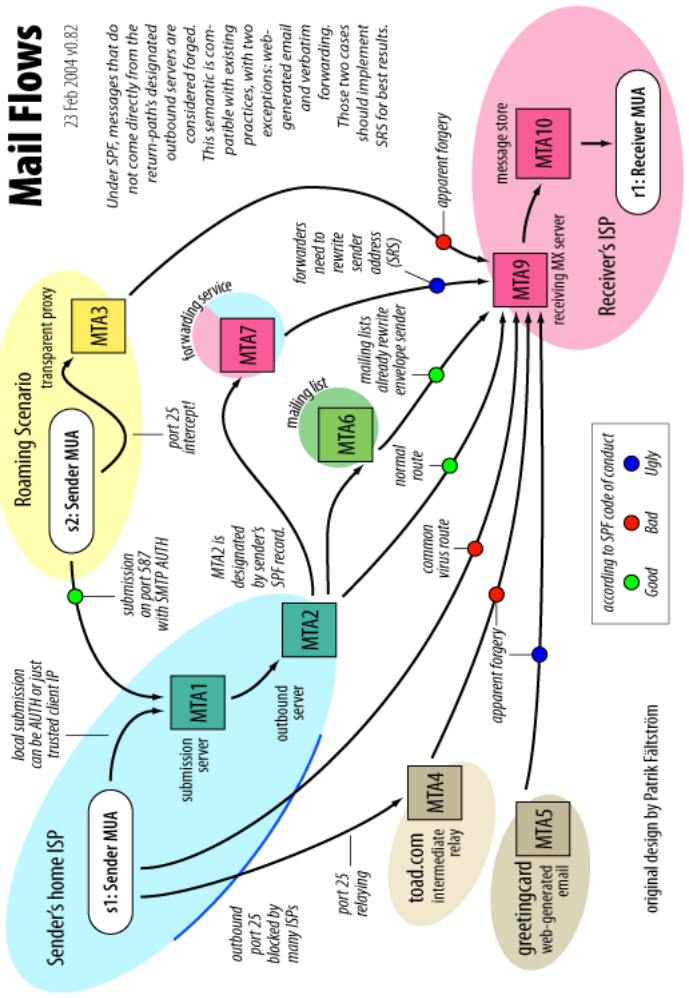
[18] P. Mockapetris, *Domain Names-Implementations and Specification*
http://www.ietf.org/rfc/rfc1035.txt
november 1987

[19] R. Braden, *Requirements for Internet Hosts – Application and Support*
http://www.ietf.org/rfc/rfc1123.txt
Oktober 1989

[20] C. Partridge, *Mail routing and the domain system*
http://www.ietf.org/rfc/rfc974.txt
Januari 1986

Bijlage A

Mail flows



Figuur A.1: Mail scenario's, http://spf.pobox.com/mailflows.html

Bijlage B

Alternatieven voor SPF

- Bonded Sender Program
  http://www.bondedsender.com/
- Trusted Sender Program
  http://www.trustedsender.com/
- Sender ID Framework
  http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx
- Trusted-Class Email
  http://www.goodmailsystems.com/
- Trusted Email
  http://imsc-dmim.usc.edu/publications/TrustedEmail.pdf
- Sender ID Solution
  http://www.clickz.com/features/insight/article.php/3391481
- DomainKeys
  https://www.sendmail.com/smi/news/pressrelease.jsp?eventOID=80351&localId=USA