专题研究报告（二）

邮件发送者政策框架及其应用

姓　　名：徐　激

学　　号：030963

导　　师：龚　俭

邮件发送者政策框架及其应用

徐激[1]　陈巍　龚俭

（东南大学计算机科学与工程系　南京 210096）

【摘要】伪造邮件发送方地址是垃圾邮件发送者的惯用手法，这给垃圾邮件的定位和过滤带来了很大的不便。邮件发送者政策框架（SPF）的是一个 SMTP 协议的辅助协议，从而能够消除垃圾邮件的伪造问题。本文描述了邮件发送者政策框架的原理、工作过程和它的发展状况，详细讨论了 SPF 的实际应用方法，并针对转发邮件的 SPF 应用中所产生的特殊问题给出了可行的解决方法。

【关键词】邮件发送者政策框架；垃圾邮件；简单邮件传输协议；网络安全

Sender Policy Framework and its Application

Xu Ji　Chen Wei　Gong Jian

(Southeast University, Computer Science & Engineering Dept., Nanjing, P.R.China, 210096)

【**Abstract**】Email address forgery is commonly used by spammers. This kind of forgery brings great inconvenience for positioning and filtering spam mails. Sender Policy Framework (SPF) is an assistant protocol which can help to fight email address forgery. This paper gives a description of SPF in its principle, working process, and state-of-art of its application. Its practical usage is discussed in detail. And the feasible way to solve the problems when it is applied specially in forwarding mail system is suggested.

【**Key Words**】SPF; Spam mail; SMTP; Network security

1. 引言

随着 Internet 中电子邮件的普及和发展，垃圾邮件的数量迅速增多，严重影响了用户对电子邮件的正常使用。目前，对于这些垃圾邮件的处理方法已经得到人们的广泛关注，尤其是近几年出现了很多优秀的垃圾邮件过滤技术。然而仅仅在邮件接收方被动地对邮件进行过滤，并不能彻底消除甚至抑制垃圾邮件的产生，它们仍然会越来越严重地消耗正常用户的系统资源。因此，对待垃圾邮件需要采用一种更加主动的方式，在邮件发送者这一端作好防治工作。邮件发送者政策框架（Sender Policy Framework，简称 SPF）正是通过检测发送方地址的域名来解决垃圾邮件中的地址伪造问题，从而能够很好地抑制垃圾邮件的一种方法。本文首先描述了邮件发送者政策框架的原理、工作过程和发展状况。之后，从 SPF 的发布和它的识别两方面，分别详细地讨论了 SPF 的实际应用方法，并做出评价。本文还讨论了 SPF 在转发邮件的应用中所产生的特殊问题，并针对该问题给出了可行的解决方法。

2. SPF 的概念及其工作过程

Internet 中发送邮件所使用的简单邮件传输协议（SMTP）本身存在一个安全问题，即发起 SMTP 连接的一方可以任意设置自己的地址信息。垃圾邮件发送者们常常利用这一点，伪造邮件发送方的地址，使得邮件接收方无法判定邮件中发送者地址的真实性。同时，由于邮件发送方地址不可信，邮件管理员很难利用黑名单等方式过滤不受欢迎的邮件，也无法给予一定的警告性回击，例如退信等。但是，SMTP 协议在 Internet 中已经被广泛使用，对该协议做重大的改动或者彻底替换是不可行的，因此一些用于辅助 SMTP 进行源地址认证的

---

[1]作者简介：徐激，女，硕士研究生，主要研究方向为网络安全；陈巍，男，硕士研究生，主要研究方向为网络信息集成；龚俭，工学博士，东南大学计算机系教授、博导，主要研究方向包括网络管理、网络安全、网络行为学、网络体系结构等。

方法相继被提出。除了 SPF 以外，还包括 Gordon Fecyk 提出的指定发送者协议（Designated Mailer Protocol,，DMP）[5]，Hadmut Danisch 提出的反向邮件交换协议（Reverse MX，RMX）[6]，以及 Yahoo 公司提出的域名密钥的概念等。这其中，SPF 涵盖了 DMP 和 RMX 的特征，并以其简单、灵活、可扩展的特性得到了较好的评价。

SPF 利用 DNS 的传输机制，通过在 DNS 信息中增加 SPF 记录，来帮助邮件接收者识别邮件发送方域名的真伪。SPF 的工作过程包括两个部分：1）DNS 中发布 SPF 记录；2）邮件接收方做 SPF 记录的识别。

第一方面，域管理员在所管辖的 DNS 中发布 SPF 记录，用于指明本域中发出邮件的地址信息，即邮件地址中由本域名结尾的邮件应该所处的 IP 地址范围。

正常邮件中，在 99%的情况下[3]，以某一域名结尾的邮件应当来自于相对固定的几台服务器上。无论域的大小，可能产生邮件的 IP 地址范围总是有限的。例如，gnu.org 结尾的邮件应当来自于 gnu 组织的服务器中，且这些服务器的 IP 地址是相对固定的。在现有的 DNS 传输机制中，接收邮件服务器以 MX 记录标明，用来寻找接收邮件的服务器地址。而发出邮件所使用的服务器有可能与 MX 记录一致，但也有可能不一致，例如发送方地址以 gnu.net 结尾的邮件可能是从 gnu.org 域的服务器上发出的。因此，从 DNS 中的 MX 记录并不能确定某域中用来发出邮件的服务器的 IP 地址范围，这就需要该域的管理者以一种简单、公开的方式声明本域可能产生邮件的 IP 地址范围，即 SPF 记录。

另一方面，邮件接收方通过 SPF 记录来识别邮件地址的真实性，所有 From 地址以某域名结尾但交互对方 IP 地址并不是处在 SPF 所指范围内的邮件均可以认为是伪造的。邮件服务器在接收邮件过程中，进行 DNS 中的 SPF 记录查询，并判断当前交互的对方 IP 地址是否满足 SPF 记录的要求，如果不满足可以在邮件内容到达前就拒绝接收。

SPF 是在 SMTP[7]交互过程中开始工作，其详细工作过程如图 1 所示。当邮件发送者发起 SMTP 请求后，首先向接收方发出 HELO 信息，告知自己的机器名称，等待接收方进行响应。得到正常回应之后，发送方给出 MAIL FROM 信息，即邮件发送者的地址。此时接收方的 SPF 解析功能开始作用，其主要的工作对象是邮件发送者地址的域名部分。如果 MAIL FROM 中的信息是空的，则采用 SMTP 交互中先前收到的 HELO 信息作为被分析的域名对象。接收方的邮件服务器发出 DNS 请求，查询该域名的 DNS 信息。如果 DNS 信息中不包含 SPF 记录，说明该域名没有发布 SPF 记录，不能对该邮件的发送者地址作识别，返回未知状态，或继续交互；如果该域名的 DNS 信息中包含 SPF 记录，则查看当前连接的对方 IP 地址是否满足这条 SPF 记录的要求：不满足则说明对方声明的发送者地址是伪造的；如果满足 SPF 的要求，则说明发送者地址是真实的，可以返回 ok 信息继续 SMTP 数据传输。

图 1　SPF 的工作过程

3. SPF 的应用

SPF 的思想产生于 2003 年，并在 2004 年的反垃圾邮件年会中被 Eric Raymond 所表述，从而引起广泛关注。关于 SPF 的草案已经提交给 IETF，并即将成为正式的 RFC 标准。目前，SPF 得到了多个组织和公司的支持，GNU、AOL、Google 等已经在它们的 DNS 中发布了 SPF 记录。并且，一些著名的域名提供商也已声明提供 SPF 的发布功能，如 PairNIC、EasyDNS 等。同时，诸如 Symantec、Brightmail 等著名的反垃圾邮件公司已在他们的产品中增加了支持 SPF 的识别功能。可见，SPF 已经开始付诸实施，其发展速度很快。

SPF 的优越性体现在它的使用过程简单明了，而且只需要 DNS 和邮件服务的管理员参与。对于普通用户来说，是否在现有的 DNS 和 SMTP 协议中采用 SPF 是完全透明的。与 SPF 的工作过程相对应，SPF 的应用需要 DNS 和邮件服务管理员两方面的配合。DNS 中 SPF 记录的配置非常简洁，并且 DNS 管理员一旦配置好 SPF 记录就无需再做任何维护工作。邮件服务管理员则需要在其邮件传输代理（MTA）中加入 SPF 的解析功能来识别邮件发送者地址的真伪。

3.1 SPF 记录的发布

在 DNS 中发布 SPF 记录是有效应用 SPF 的先决条件。SPF 利用 DNS 记录中的 TXT 记录来承载信息。如果有一条 DNS 的 TXT 记录以“v=spf1”开头，则表明这是一条 SPF 记录，其版本号为 1。之后以空格作为间隔分别列出对应域名的 IP 地址范围。IP 地址范围的表示主要包括四种类型：A、MX、PTR、IP4，详细说明[2]如下：

- A：表示该域名所对应的 IP 地址。如果需要加上其他域名所对应的 IP 地址，则表示为 A:other.com。
- MX：表示该域名的 MX 服务器所对应的 IP 地址。如果需要加上其他域名的 MX 服务器所对应的 IP 地址，则表示为 MX:other.com。
- PTR：表示如果对方 IP 地址存在 PTR 记录，且该 PTR 记录中以该域名结尾，则该 IP 符合要求。如果需要加上以其他域名结尾的 PTR 记录所对应的 IP 地址，则表示为 PTR:other.com。
- IP4：直接表示 IP 地址，可以使用掩码的方式表示一段地址，如 192.0.1.0/24。

以上四种类型的 IP 地址范围包括了常用的邮件服务器地址的表达方式，如果需要加入新的类型可以进行扩展。例如，如果地址改为 IPv6 的格式，则可以以“IP6”来定义新的 IP 地址范围，并且不影响接收方对已有地址类型的识别。

在记录的最后，用“all”结尾表示不符合前面所有的 IP 地址范围时的默认处理方式。“-all”表示拒绝接收邮件；“?all”表示中立，即可以当作没有 SPF 记录的情况处理，由于目前 SPF 的工作刚刚起步，大多数公司和组织所发布的 SPF 记录仍是以?all 结尾的；“~all”表示虽然不符合 IP 地址范围的要求，但并不保证邮件发送者地址一定是伪造的，这也是过渡阶段为防治潜在的错误所制定的一条可选配置。

以某校园网的域名“myuniversity.edu.cn”为例，该域名的 DNS 管理员需要在配置文件中增加一条 TXT 记录：

myuniversity.edu.cn　　TXT　　“v=spf1　mx　?all”

这条 SPF 记录以 MX 的方式指明了可能产生 myuniversity.edu.cn 结尾的邮件服务器 IP 地址范围，即以该域名结尾的邮件只有可能从 MX 所指的邮件服务器发出。这样，在查询 myuniversity.edu.cn 域名信息的返回结果中就可以得到如下信息：

myuniversity.edu.cn　　text=”v=spf1　mx　?all”

myuniversity.edu.cn　　MX preference = 0, mail exchanger = mail.myuniversity.edu.cn

……

mail.myuniversity.edu.cn　　internet address = 192.168.0.10

第一条 text 记录即为 DNS 所发布的 SPF 信息，”v=spf1”表示这是一条 SPF 记录，”mx”表示该域发出邮件的 IP 地址是其 MX 服务器的 IP 地址。由第二条记录和最后一条记录可以得知，该域名的 MX 服务器的 IP 地址为 192.168.0.10（此处为虚拟的 IP 地址）。因此，对于邮件接收者而言，如果邮件中的发送方地址以 myuniversity.edu.cn 结尾，但交互对方的 IP 地址并非 192.168.0.10，则可以认为其发送者地址是不真实的。

3.2 邮件服务器的 SPF 识别

当多数 DNS 信息中发布了 SPF 记录后，邮件管理员就可以从 SPF 的主页上下载并安装 SPF 插件，来自动过滤伪造地址的邮件了。SPF 的先导者们已经在他们的主页上给出了诸如 Sendmail、Postfix、Qmail 等多种邮件传输代理软件的插件代码，帮助邮件管理员解决 SPF 的识别问题[1]。插件代码的主要作用是在邮件服务器接收邮件时，检查对方声明的域名是否发布了 SPF 记录，如果是则比较交互对方的 IP 地址是否处于 SPF 记录所指明的 IP 地址范围，从而决定是否继续接收邮件。

在 CERNET 中，多数校园网的邮件服务器仍然使用 Sendmail 作为邮件传输代理软件。以此为例，作者安装适用于 Sendmail 的插件代码来识别和解析 SPF 记录。

该插件代码是用 Perl 语言编写，需要 Perl5.8 或以上版本的支持，具体的安装步骤如下：

1）下载插件 sendmail-milter-spf-1.41.pl，如果是 RedHat Linux 系统可以直接使用 rpm 安装包。

2）安装 Perl5.8.x

3）安装 Perl 的所需支持模块，包括：

perl(Sendmail::Milter)
perl(Mail::SPF::Query)
perl(Mail::SRS)
perl(Net::CIDR)

4）配置 Sendmail 的插件功能，以支持该插件。在其配置文件中加入如下内容：

```
define(‘confMILTER_LOG_LEVEL’,‘9’)dnl
define(‘confMILTER_MACROS_HELO’,‘confMILTER_MACROS_HELO’,‘{verify}’)dnl
INPUT_MAIL_FILTER(‘spf-milter’,‘S=local:/var/spf-milter/spf-milter.sock,F=T,T=C:4m;S:4m;R:8m;E:10m’)
```

5）启动插件的 SPF 识别进程

perl /usr/local/spf/sendmail-milter.pl milter（也可改为其它已存在的用户名启动进程）

6）重新启动 Sendmail

对于其它邮件传输代理，如 Postfix、Qmail 等也可以下载相应的插件代码进行安装。这样在邮件服务器这一端就可以通过解析 DNS 信息中的 SPF 记录，来识别和判断邮件发送方声明的地址信息。

3.3 SPF 应用的评价

SPF 本身虽然并不能完全过滤垃圾邮件，但是它可以解决邮件发送过程中的地址伪造问题，因此 SPF 的广泛应用可以很好的抑制甚至消除垃圾邮件的产生，对于 Internet 的邮件系统而言具有长远的利益。

首先，SPF 可以保证发送方地址的真实性，对于邮件管理员来说，就可以根据地址中的域名来定位邮件的发送者，结合使用黑白名单算法来过滤垃圾邮件和保护正常邮件将变得可行和有效得多。其次，即使垃圾邮件发送者们转为使用虚假域名，或者没有发布 SPF 记录的域名，其所能使用的地址域名将非常有限，并会逐渐减少，这对长期抑制垃圾邮件将会有很大效果。最后，由于邮件发送方地址是在 SMTP 交互过程中进行识别的，因此对于伪造地址的邮件可以在邮件数据没有到达本地之前就直接拒收，从而明显减少接收方系统资源的

消耗。垃圾邮件发送者中，对于普通使用者而言，会因为邮件被拒收产生大量的系统警告信，因此他企图发送的越多，所产生的资源耗费就会越多；而对于专业使用者来说，SPF 也可以有效制止其行为。例如，垃圾邮件发送者通常会采取一种字典攻击的方式，在 RCPT TO（接收方地址）的交互中不断改变字符串内容来探测对方邮件服务器上已存在的用户名。由图 1 可见，MAIL FROM（发送方地址）交互是在 RCPT TO（接收方地址）交互之前发生的，因此如果在接收到 MAIL FROM 信息后能够利用 SPF 有效识别发送方地址，就可以制止这种字典攻击。

总的来说，SPF 的应用将是正常的邮件使用者对垃圾邮件发送者的一次很好的回击。如果接收者只是被动地在接收方一端过滤垃圾邮件，那么无论过滤技术如何先进都不能避免垃圾邮件的产生。Internet 的邮件系统只有不断地完善，弥补 SMTP 协议本身的安全缺陷，缩小垃圾邮件所能够产生的空间，才能从根本上彻底地消除垃圾邮件。

4. 转发邮件的 SPF 应用

但是，SPF 与现有的两类邮件发送体制产生了矛盾，是目前亟待解决的问题。一类是系统转发的邮件，另一类是由网页产生的邮件。无论是转发邮件还是由网页产生邮件的情况，均是在发送邮件时利用了 SMTP 缺乏发送方认证的弱点虚报发送方信息，来简化邮件的处理过程。虽然这种虚报并非恶意伪造，但与 SPF 的要求相违背，因此需要做出改动以适应这种变化。本节将详细讨论转发邮件的 SPF 应用。

由于系统在转发邮件时通常不改变邮件中的发送者信息，但邮件发送方的 IP 地址却变成了转发服务器的 IP 地址，因此被转发的邮件在 SPF 识别时会被认为是地址伪造的。在 UNIX 系统中使用邮件代理软件的.forward 或者 aliases 文件的别名功能对邮件进行转发均会产生这样的问题。为此出现了发送者地址重写方案（Sender Rewriting Scheme，SRS）[4]，即转发系统在转发邮件前先封装原先的邮件发送方地址，再以自己的地址发送邮件。如果邮件被弹回，系统解封装原先的地址后再退回给原始的邮件发送者。目前，最新的 SPF 开源代码中增加了邮件服务的 SRS 功能，邮件服务公司 Pobox 也已经在其转发邮件系统中支持 SRS。

但是在 SPF 被采用的过渡阶段，要求所有的转发邮件服务器安装支持 SRS 的插件是不可行的。因此，需要一种更加简便的方式实现邮件转发时的地址识别问题。以下是一封邮件的标准内容：

```
From sendername@sender.com
Return-Path: sendername@sender.com
……
From: sendername@sender.com
Reply-To: sendername@sender.com
To: receivername@receiver.com
Subject: test mail
    This is a test mail.
```

对照图 1 中邮件的发送过程，这封邮件的前两行内容是由“MAIL FROM”交互产生的，也正是 SPF 工作的对象。后面的内容是由“DATA”交互产生的，包括其中的 From 和 Reply-To 等信息，它们与 SPF 的工作无关，是为邮件用户代理（MUA）所使用的。由此可见，当系统转发一封邮件时，只要保证“MAIL FROM”交互时的地址符合 SPF 要求，就不会被邮件接收方误判。假设转发邮件服务器域名为“forwarder.com”，它仅在“MAIL FROM”交互中声明自己真实的域名，而在“DATA”交互中保留邮件的原始信息，则转发后的邮件内容为：

```
From forwardername@forwarder.com
Return-Path: forewardername@forwarder.com
```

……

From: sendername@sender.com

Reply-To: sendername@sender.com

To: receivername@receiver.com

Subject: test mail

This is a test mail.

本文选用 procmail 来实现这种转发机制。Procmail 是一个自动化的邮件处理软件包，能够通过多种方式对邮件进行预处理。Procmail 的使用非常普及，大多数 Linux 系统都默认地自带这个软件包。利用它进行邮件转发，只需要在用户主目录下面建立.procmailrc 文件，其内容为：

:0

! receivername@receiver.com

表示所有邮件转发至 receivername@receiver.com。Procmail 与 aliases 等别名转发方式的机制不同，它在转发用户邮件时，是以服务器的真实身份与邮件接收方交互，不改变的是邮件内容中的发送者信息，因此不会产生被误判的情况。当转发邮件发生错误时，邮件转发服务器根据信件中的原始发送者信息给与退信。而当接收者正常回信时，MUA 会直接从邮件内容中的 Reply-To 信息中找到直接可以回复的地址，并不需要通过转发服务器。因此，在普及 SPF 的过程中，鼓励使用 Procmail 进行邮件转发是一个简单可行的选择。

5. 结束语

在目前没有统一的邮件发送方认证标准的情况下，SPF 应运而生，并很快得到了广泛的关注。SPF 简单易用，对用户完全透明，在过渡时期能够很好地适应各种变化过程。相对来说，它对现有的邮件系统产生的冲击很小，并且具备良好的扩展性。SPF 的广泛应用，可以有效地解决邮件中的发送方地址伪造问题，完善 Internet 邮件系统本身的缺陷，从而从根本上消除垃圾邮件。

然而，采纳 SPF 的过程，并不一定是完全平滑的，它需要所有 DNS 管理员以及邮件服务管理员的积极参与，也需要改变一些特殊邮件服务（转发邮件和网页产生的邮件）的机制。尤其是由网页产生的邮件，其随意性更大，需要根据具体的情况做改动，有待进一步的改进。但是，相对于垃圾邮件给正常用户和反垃圾邮件者带来的耗费来说，这些变化应该是可以接受的。

参考文献

[1] http://spf.pobox.com/, SPF's Home Page

[2] Mark Lentczner, Meng Weng Rong, Sender Policy Framework (SPF), A Convention to Describe Hosts Authorized to Send SMTP Traffic, draft-mengwong-spf-01.txt, May 2004

[3] Meng Weng Wong, SPF Overview, http://www.linuxjournal.com, April 01, 2004

[4] Meng Weng Wong, SPF, MTAs and SRS, http://www.linuxjournal.com, May 01, 2004

[5] Gordon Fecyk, Designated Mailers Protocol, draft-fecyk-dmp-02.txt, May 2004

[6] Hadmut Danisch, The RMX DNS RR and method for lightweight SMTP sender authorization, draft-danisch-dns-rr-smtp-03.txt, Oct 2003

[7] J. Klensin, Editor, AT&T Laboratories, Simple Mail Transfer Protocol, RFC2821, Apr 2001