SPF 技术在邮件服务系统中的应用

Application of SPF in the mail server system

蓝炳伟 （南开大学 300071）

摘要：电子邮件是 Internet 应用最广的服务；通过网络电子邮件系统，您可以用非常低廉的价格，以非常快速的方式，与世界上任何一个角落的网络用户联络。但是，垃圾邮件也随着互联网的不断发展而大量增长，垃圾邮件的危害现在已经深入人心。本文主要介绍 SPF 技术在邮件服务系统中的应用，达到阻止垃圾邮件的目的。

关键词：邮件系统 SPF 垃圾邮件

1 引言

现代网络技术的高速发展，特别是 Internet 的日益普及，推动了各种网络应用服务的发展。作为网络应用最为重要的应用之一，E－mail 服务跨越了地域及空间的制约因素，为广大的使用者创造了良好的条件。同时产生的垃圾邮件也给互联网以及广大的使用者带来了很大的影响，这种影响不仅仅是人们需要花费时间来处理垃圾邮件、占用系统资源等，同时也带来了很多的安全问题。本文主要介绍 SPF 技术在邮件系统中的应用，从而达到阻止垃圾邮件的目的。

2 SPF 简介

2.1 SPF 概述

SPF 是发送方策略框架（Sender Policy Framework）的缩写，是一种以 IP（互联网协定）地址认证电子邮件寄件人身份的技术。SPF 诞生于 2003 年，它的缔造者 Meng Weng Wong 结合了反向 MX 域名解析和 DMP（Designated Mailer Protocol）的优点。SPF 很容易使用，不管是一家 ISP，商业机构，一所学校，或者一个虚拟主机，只要在 DNS 中发布一条 SPF 记录，告诉尝试给你的邮件服务器发送邮件的其它服务器："我只从这些机器发送邮件，如果其它任何机器声称是从我这里发送的邮件，那么它们一定是假的！"。例如：abc. com 是发件人域，sohu. com 是收件人域。假如 abc. com 的一个真实发件人给 sohu. com 发送一封邮件，sohu 检查 abc 的 SPF 记录，以确定这封邮件是否是从 abc 许可的机器上发送的。（这封邮件的来自的 IP 地址是否在 abc 的 SPF 记录中）。如果是，则 sohu 将允许这封邮件通过。相反，若有人假冒 abc 发送邮件给 sohu，sohu 检查 abc 的 SPF 记录，发现发件者 IP 并不再记录中，这封邮件将被阻断。

2.2 SPF 记录的格式简介

随着 SPF 技术的广泛应用，越来越多的大公司及 ISP 都在 DNS 中配置了 SPF 记录，从而阻止了别人假冒自己的域名来发垃圾邮件。在 DNS 中，SPF 的 TXT 记录格式如下：

v = spf1 [[pre] type [ext]] ... [mod]

每个参数的含义如下表所示：

3 SPF 在邮件系统中的应用

基于 SPF 技术，邮件服务器监听进程（MTA）只要在接收到 MAIL FROM 命令后，向 DNS 服务器发送请求 SPF 记录得到该域名的相应的 IP 地址，然后和监听到的 IP 进行比较就知道发送者是否假冒者了，从而可以阻止其继续发送邮件（见如图 1）。

如图所示，首先，邮件系统 MTA 监听客户端连接，并获取客户端 IP 地址，HELO 命令值，MAIL FROM 命令值（获得发送方的域名），然后发送一个 DNS 请求获取发送方域名的 SPF 记录，如果该域名没有 SPF 记录，则继续 MTA 的其它流程，如果该域名存在 SPF 记录（比如"v = spf1 a mx －all"），则依次检测 SPF 记录项（上例中有 a，mx，－all），如果是 a，则又向 DNS 发送一个请求获取 A 记录，然后看 A 记录里包含有客户端 IP 地址没，如果包含，则表示真实邮件客户端，继续 MTA 的

其它流程，否则继续根据 SPF 记录项依次比较（mx，-all），如果到最后一项 - all 还没有匹配上客户端 IP 地址，则可认为此客户端是假冒别的域在发垃圾邮件，从而 MTA 可立即拒收该 IP 地址发过的邮件，这样就可从源头上大大减少了垃圾邮件的产生。

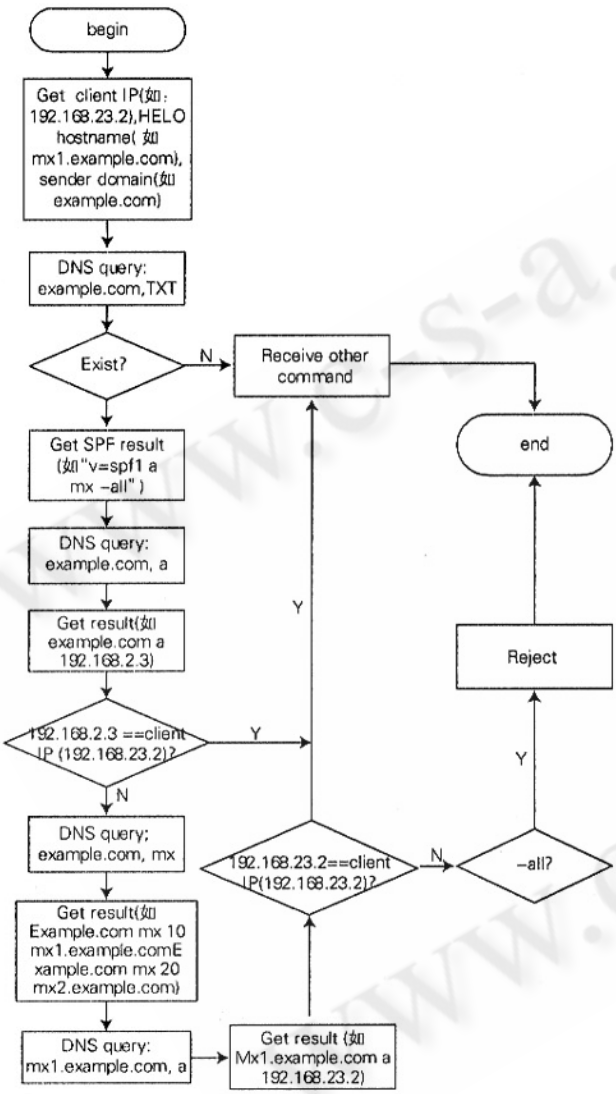

图 1　MTA 查询 SPF 记录过程图

4　总结

本文简要介绍了 SPF 技术，并阐述了在邮件服务系统中的如何应用 SPF 技术，很好地解决了传统的邮件服务系统中的域名被欺骗而产生的垃圾邮件问题，有效的减少了垃圾邮件的产生。

参数	描述
v=spf1	SPF 的版本。
pre	定义匹配时的返回值。 可能的返回值包括： 返回值　描述 +　缺省值。在测试完成的时候表示通过。 -　表示测试失败。这个值通常是 -all，表示没有其他任何匹配发生。 ~　表示软失败，通常表示测试没有完成。 ?　表示不置可否。这个值也通常在测试没有完成的时候使用。
type	定义使用的确认测试的类型。 可能的值包括： 候选值　描述 include　包含一个给定的域名的测试 以 include:domain 的形式书写。 all　终止测试序列。 比如，如果选项是 -all，那么到达这条记录也就意味着测试失败了。但是如果无法确定，可以使用"?all" 来表示，这样，测试将被接受。 ip4　使用 IPv4 进行验证。 这个可以以 ip4:ipv4 或 ip4:ipv4/cidr 的形式使用。建议使用这个参数，以减少域名服务器的负荷。 ip6　使用 IPv6 进行验证。 a　使用一个域名进行验证。 这将引起对域名服务器进行一次 A RR 查询。 可以按照 a:domain，a:domain/cidr 或 a/cidr 的形式来使用。 mx　使用 DNS MX RR 进行验证。 MX RR 定义了收信的 MTA，这可能和发信的 MTA 是不同的，这种情况基于 mx 的测试将会失败。 可以用 mx:domain，mx:domain/cidr 或 mx/cidr 这些形式进行 mx 验证。 ptr　使用域名服务器的 PTR RR 进行验证。 这时，SPF 使用 PTR RR 和反向图进行查询。如果返回的主机名位于同一个域名之内，就验证通过了。 这个参数的写法是 ptr:domain exist　验证域名的存在性。 可以写成 exist:domain 的形式。
ext	定义对 type 的可选扩展。如果没有这个字段，那么仅使用单个记录进行问询。
mod	这是最后的类型指示，作为记录的一个修正值。 修正值　描述 redirect　重定向查询，使用给出的域名的 SPF 记录。 以 redirect=domain 的方式使用。 exp　这条记录必须是最后一条，允许给出一条定制的失败消息。 IN TXT " v=spf1 mx -all exp=getlost.example.com" getlost IN TXT " You are not authorized to send mail for the domain"

参考文献

1 Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL(V1)2005.

2 http://www.openspf.org/