反垃圾邮件技术简述

何飞

1 引言

电子邮件现在已经发展成为公司、机构以及社会网络（Social Networks）中标准的通讯方式。电子邮件由于其接近即时传输的便捷性以及极低的成本而得到广泛的应用。但它的优点在促进电子邮件作为一种重要的通讯媒介的同时，也导致了相当严重的误用和滥用。发送电子邮件的低成本，促使一些机构或个人向他们能发送的任何人发送未索取的商业信件。这种未索取的信件，称为垃圾邮件，已日益严重。据中国互联网络信息中心（CNNIC）2005 年 7 月发布的《中国互联网络发展状况统计报告》显示，中国网民人均每周收到 5.2 封正常邮件，9.3 封垃圾邮件，垃圾邮件占了总邮件数量的 64.7%。如此泛滥的垃圾邮件，促使各种反垃圾邮件技术被研究出来，来高效准确地阻止垃圾邮件。

2 垃圾邮件的发送技术

2.1 用 Webmail 服务

垃圾邮件发送者一个常用的方法是在免费的 Web 邮件服务，比如 Hotmail，注册许多帐号，用这些帐号来发送垃圾邮件或者接受他们的潜在客户的邮件。由于垃圾邮件发送者需要发送大量的邮件，所以一般他们需要大量邮件帐号，他们会用 web bots 这种程序来自动创建这些帐号。

为了阻止这种方式的滥用，现在几乎所有的 Web 邮件服务提供商都采用了一种被称为 captha 的系统：每个企图创建一个新帐号的用户会被要求将一个在复杂背景上有着几个奇怪字符的图案中的字符识别出来。人可以比较容易的识别这些字符，但对于计算机程序来说，至少现有的标准的 OCR 技术很难识别出这些字符。对于盲人用户，一些网站会提供一段音频，要求识别其中的字符。

2.2 通过其他人的计算机

2.2.1 利用中继转发

早期，很多邮件服务器都提供开放中继（Open Relay）功能。该功能允许转发所有的入站邮件，而对该邮件的发送和接收者是否是本邮件系统用户不进行检查。所以早期的垃圾邮

件发送者一般就利用打开开放中继的邮件服务器作为中转站来发送垃圾邮件。

2.2.2 开放代理

最近几年，大多数的邮件发送代理（mail transport agent, MTA）都已经关闭的 Open Relay 功能，而且采用了需要认证的 ESMTP 协议。垃圾邮件发送者开始诉诸于其他手段，其中最显著的一种是利用公开的代理服务器。

公开代理是指一个为任意客户端创建联通任何服务器，而不需要认证的代理服务器。像早期的开放中继一样，现在的开发代理服务相对来说是很常见的。一个垃圾邮件发送者可以通过一个开放代理服务器连接一个邮件服务器，然后发送垃圾邮件。由于邮件服务器只会记录来几代理服务器的连接，而不是垃圾邮件发送者的计算机，这种方法比利用开放中继提供了更好的隐秘性。

2.2.3 垃圾邮件病毒

从 2003 年开始，垃圾邮件的调查者们发现，垃圾邮件发送者发送垃圾邮件的方式有了一个根本性的改变。垃圾邮件发送者开始创建自己的“服务”，而不是满世界搜寻类似于开放中继和开放代理。通过传播可以部署代理服务器或邮件发送服务器的恶意代码，垃圾邮件发送者可以利用成千上万的受害主机来发送垃圾邮件[1]。

2003 年爆发的主要的 Windows 上的邮件病毒，包括 Sobig 和 Mimail，都属于垃圾邮件病毒：这些病毒使得感染的主机迅速成为一个发送垃圾邮件的工具[2][3]。

除了发送垃圾邮件，垃圾邮件病毒对于垃圾邮件发送者来说还有另外的作用。从 2003 年 6 月开始，垃圾邮件发送者开始用一些类似的病毒对 DNSBL 等反垃圾邮件资源实施分布式拒绝服务（distributed denial-of-service, DDoS）攻击。[4]

3 反垃圾邮件技术

3.1 源地址过滤

源地址过滤一般部署在邮件传输代理上，是一种针对发件服务器的基于 IP 地址的过滤，主要有白名单、黑名单两种。

3.1.1 白名单（Whitelist）技术

在垃圾邮件过滤中，白名单指的是一个可信的放送方的列表。邮件传输代理将从这个列表中的 IP 地址收到的邮件直接投递到用户的邮箱中，而可以不做其他方式的过滤。事实上，白名单也可以不仅仅是基于 IP 的，也可以是基于发件人的邮件地址。但这时候就会涉及到发件人伪造的问题，由于 SMTP 协议的不安全性，垃圾邮件发送者可以伪造成一个在白名单中的邮件地址来发送垃圾邮件。这个问题就需要下一节中介绍的发件方认证技术来解决。

3.1.2 黑名单（Blacklist）技术

黑名单恰好与白名单相反，邮件传输代理从黑名单中接受到的邮件会直接被过滤掉。现在的邮件传输代理一般都支持 Domain Name System Blackhole List (DNSBL)。DNSBL 是一个实时的垃圾邮件源或中继的 IP 地址。第一个 DNSBL 是 Paul Vixie 为 Mail Abuse Prevention System (MAPS) [5]创建的 Real-Time Blackhole List (RBL)。Spamhaus[6]的 Spamhaus Block List (SBL)和 Spamhaus Exploits Block List (XBL)是现在使用最广泛的 DNSBL 了。

DNSBL 系统构建在域名解析系统之上，下面举例说明一个实现了 DNSBL 的邮件服务器的工作流程。假设邮件服务器 A 采用的是 sbl.spamhaus.org 提供的 DNSBL 服务，当 A 收到一个 IP 地址为 a.b.c.d 的发件方的连接请求时，会把这个 IP 地址添加到 DNSBL 服务器的域名之前，形成这样的域名 d.c.b.a.sbl.spamhaus.org。然后用 DNS 反查这个域名对应的 IP 地址，如果 DNS 纪录返回的是一个 IP 地址，说明这个发件方在黑名单中，连接请求直接被拒绝。

总的来说，基于 IP 地址过滤的方案可以解决一部分的问题。但这种方案的缺点也是显而易见的：IP 地址空间过于庞大；对于采用动态域名的垃圾邮件发件人，很难进行过滤；对于利用垃圾邮件病毒（botnet）的发送者，无法进行有效过滤等。

3.2 发送方认证

3.2.1 质询与应答（Challenge/Response）[7]

质询与应答系统是一种和白名单结合使用的系统，发送方需要手动的将自己加到接受方的白名单中去。当接受邮件服务器从一个不在白名单中的邮件地址收到一封邮件时，会自动发回给发件人一封质询，当发件人正确回复这封邮件后，邮件服务器会将此发件人加入到白名单中。

Challenge/Response 的变种有 Human Interactive Proofs (HIP)[8]、Proof of Work（PoW）[9]、Micropayments 等，这些方案都基于这样的思想：增加发送方的负担；增加垃圾邮件发送者的发送成本等。

质询与应答系统存在的缺陷主要有以下几点：第一，对于邮件列表（maillist）这种应用，由于从邮件列表发来的邮件是不可能得到应答的，所以需要邮件服务器的管理员手动将邮件列表的地址加入白名单中；第二，如果发送方和接受方都不在双方的白名单中，则会形成 challenge-response 死锁；第三，由于质询与应答系统没有验证发件人地址的真实性，还是伪造在白名单中的发件人来发送垃圾邮件。

3.2.2 邮件认证（Email Authentication）

邮件认证是一种收件人用来确认发件人身份的机制。SMTP 协议[10]最大的弱点在于，发件人的地址可以非常容易地进行伪造，这个问题的存在使得现有的很多解决方案都存在一定的漏洞。为了解决这个问题，业界很多大的厂商都试图设计新的用于邮件认证的协议，并使

其成为 IETF 的标准。

现有的邮件认证的方案可以分为两类：基于 IP 地址的认证和基于加密的认证。

基于 IP 地址的认证，主要有两种协议：Pobox 公司的 Sender Policy Framework (SPF)[11] 和 Microsoft 公司从 SPF 发展而来的 Sender ID Framework (SIDF)[12]]。在 SPF 提案中，每个域名需要通过 DNS 的 TXT 纪录发布自己的 SPF 纪录，在 SPF 纪录中说明可以以这个域名发送邮件的邮件服务器的地址。例如 tinghua.edu.cn，可以在 DNS 中加入如下纪录”v=spf2.0/pra ptr mx:202.112.57.8 mx:gmail.com mx –all”，表明所有发件人地址是 somebody@tsinghua.edu.cn 邮件一定是从 202.112.57.8 或者 gmail.com 发送的。

邮件接受服务器接受到一封邮件时，只需要从 DNS 反查邮件 Mail From 域中声称的发件人的域名，得到的 spf 纪录，将 spf 纪录中允许的发件服务器地址与实际的发件服务器的地址进行对比。如果不符合，就可以认为邮件的发件人地址是伪造的，而拒绝接受这封邮件。（见图 1）

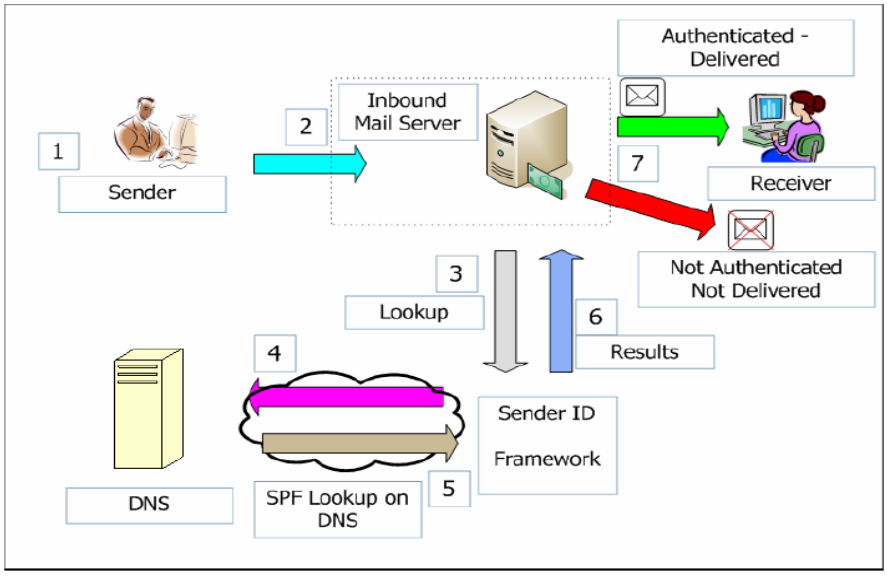

图 1 SPF 协议的处理流程示意

基于加密的邮件认证，主要也有两种：Cisco System 公司的 Identified Internet Mail (IIM)[13] 和 Yahoo!公司的 DomainKeys (DK)[14]。IIM 和 DK 最近进行了合并，形成了一个新的草案 Domain Keys Indentified Mail Standard (DKIM)[15]。

基于加密的邮件认证的基本工作方式见图 2，每个邮件服务器拥有一对公钥和私钥，邮件服务器通过 DNS 纪录发布自己的公钥。邮件服务器发送邮件时会用自己的私钥对邮件进行签名，收件服务器根据 Mail From 域中的域名从 DNS 纪录中得到发送服务器的公钥，用此公钥验证验证邮件中的签名，验证通过说明发件人的地址不是伪造的。

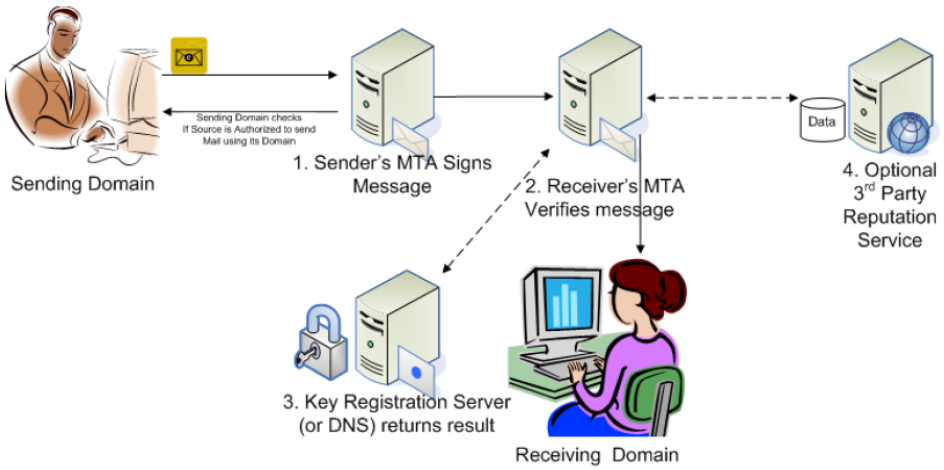

图 2 DomainKeys 协议的处理流程示意

邮件认证如果得到全面的部署，应该能很好的解决发件人伪造的问题。但这些方案也各自存在一些问题：首先，这些方案只在绝大多数的邮件服务器都支持时才能真正的得到应用。另外，对于 SPF 方案来说，最大的问题是，对于转发的邮件会产生无法通过验证的问题，要解决这个问题需要对 SMTP 协议进行扩展；Sender ID 解决了这个问题，但由于增加了对邮件体中头部（Header）中的发件人域（From）的认证，所以还需要在邮件客户端（Mail User Agent, MUA）中进行一些修改；Sender ID 的另外一个问题是，由于 Sender ID 是 Microsoft 公司的专利，很多有名的开源项目已经宣称由于不能接受 Microsoft 的授权协议，不能在项目中实现 Sender ID 协议，这其中包括著名的 Debian Project[16]和 Apache Software Foundation[17]。DomainKeys 这类的基于加密的方案，最容易遭到大家诟病的则是加密造成的对邮件服务器性能的影响。

3.3 基于内容的过滤

对于内容的过滤，现在已经有一些比较成熟的方案。主要有两大类，基于统计的邮件过滤系统和基于规则的邮件过滤系统，两者的代表分别是 SpamProbe[18]和 SpamAssassin[19]。这两类方案都已经比较成熟，这里就不详细介绍其原理，只对两者进行以下比较。

基于统计的过滤系统的优势在于，这种系统可以针对用户特定的邮件进行学习，生成分类器，一个针对特定用户的基于统计的系统经过一段时间的学习后往往可以获得比基于规则的系统更好的垃圾邮件识别率和更低的误判率。基于规则的过滤系统的优势是，可以很方便的进行部署，只需要将特定的规则集导入系统就立刻可以开始过滤工作，不需要基于统计的系统的初始学习过程。

另外还有一种比较特殊的基于校验和（Checksum Based）的过滤系统，这种方法主要优势在于可以方便的共享垃圾邮件的特征，应用于分布式的合作过滤系统中，商用的方案有 Distributed Checksum Clearinghouse[20]，Razor[21]则是开源项目中的杰出代表。

4 结束语

垃圾邮件作为一种网络上的无用信息，严重地影响了邮件系统的使用效率，许多行之有效的反垃圾邮件技术已经投入使用少{取得了一定的效果。但技术的发展从来就是彼此推进的，垃圾邮件发送技术与反垃圾邮件技术之间的较量还将继续下去。

反垃圾邮件同时也是一个社会问题，在与垃圾邮件发送者进行技术较量的同时，也需要完善法律法规，以便从法律上来威慑和惩罚垃圾邮件的制造者和传播者，减少垃圾邮件的产生源。

参考文献：

1．E-mail Spam on Wikipedia https://secure.wikimedia.org/wikipedia/en/wiki/E-mail_spam

2．http://www.cnn.com/2003/TECH/internet/08/22/sobig.culprit/

3．http://www.infoworld.com/article/03/07/11/HNtorjanpeddle_1.html

4．http://www.spamhaus.org/news.lasso?article=13

5．Mail Abuse Prevention System. http://www.mail-abuse.com

6．The Spamhaus Project. http://www.spamhaus.org

7．Example: Opensource, “Active Spam Killer (ASK)”, http://www.paganini.net/ask

8．Rachna Dhamija and J. D. Tygar. Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks. In In Human Interactive Proofs: Second International Workshop (HIP 2005), pages 127–141, 2005. http://www.cs.berkeley.edu/tygar/papers/Phish_and_HIPs.pdf

9．C. Dwork and M. Naor. Pricing via Processing or Combatting Junk Mail. In Proceedings of CRYPTO’92, Lecture Notes in Computer Science 740, pages 137–147, 1992. http://research.microsoft.com/research/sv/PennyBlack/junk1.pdf

10．IETF RFC 822, RFC 2822

11．Sender Policy Framework (SPF) for Authorizing Use of Domains in EMAIL, version 1. http://www.ietf.org/internet-drafts/draft-schlitt-spf-classic-02.txt

12．Sender ID: Authenticating E-Mail. http://xml.coverpages.org/draft-ietf-marid-core-03.txt

13．Identified Internet Mail. http://www.identifiedmail.com/draft-fenton-identified-mail.txt

14．Domain-Based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys). http://www.ietf.org/internet-drafts/draft-delany-domainkeys-base-02.txt

15．DomainKeys Identified Mail (DKIM). http://mipassoc.org/dkim/specs/draft-allman-dkim-base-00-10dc.txt

16．Debian project unable to deploy Sender ID: www.debian.org/News/2004/20040904

17．ASF Position Regarding Sender ID: http://www.apache.org/foundation/docs/sender-id-position.html

18．Opensource: SpamProbe http://spamprobe.sourceforge.net/

19．Opensource: SpamAssassin http://spamassassin.apache.org/

20．Distributed Checksum Clearinghouse: http://www.rhyolite.com/anti-spam/dcc/

21．Opensource: Razor: http://razor.sourceforge.net/

22．Kaiesh Vohra, The Identification of Unsolicited Electronic Mail, 2005:

http://www.kaiesh.com/anna/KaieshVohra2005-Antispam.pdf
23. Antispam Approaches: http://www.spamhelp.org/articles/anti-spam_approaches.pdf
24. Technical responses to spam: http://www.taugh.com/spamtech.pdf