# 基于域密匙认证的反垃圾邮件技术

赵 毅
(重庆交通学院 重庆 400074)

**摘 要** 垃圾邮件的泛滥已经严重影响邮件的正常使用,由 Yahoo 和 Cisco 公司提出的 DKIM 反垃圾邮件技术,已经提交 IETF,有望成为行业标准,能较好地解决垃圾邮件问题。文章分析了目前常用的反垃圾邮件技术,详细剖析 DKIM 的工作原理,并给出在 Sendmail 邮件服务系统中应用 DKIM 的实例。

**关键词** DKIM,垃圾邮件,域名,过滤,认证

## The Technology Based on DKIM to Prevent Spam Mails

ZHAO Yi
(Chongqing Jiaotong Uiniversity, Chongqing 400074)

**Abstract** The overflow of spam mails has been severely influenced normal application of Email systems. The DKIM technology brought up by Yahoo and Cisco has been delivered to IETF and it is expected to be the industry standard properly dealing with the problems of spam emails. This article analyzes frequently used techniques and working principles of DKIM and presents examples that are applied in Sendmail service system.

**Keywords** DKIM, Spam mail, Domain, Filtration, Identification

## 1 引言

随着 Internet 的普及,电子邮件以其快捷、方便、低成本的特点得到了广泛的使用。但是随之而来的垃圾邮件也越来越猖獗,严重地影响和损害人们的工作、生活和学习。联合国贸发会议援引 Message Labs 的数据说,垃圾邮件给全球企业带来的损失高达 205 亿美元。据 IDC 调查,2000 年全球日平均发送邮件超过 100 亿封,到 2005 年将达 350 亿封以上。

垃圾邮件主要包括:商业广告、政治言论、色情邮件、蠕虫病毒邮件、恐吓、欺骗性邮件。这些垃圾邮件占用了大量网络资源。一些邮件服务器因为安全性差,管理不善,被作为垃圾邮件转发站,被警告或封掉 IP,大量消耗的网络资源使得正常的业务运作变得缓慢。随着国际上反垃圾邮件的发展,组织间黑名单共享,使得无辜服务器被更大范围屏蔽,这无疑会给正常用户的使用造成严重问题。病毒程序、黑客攻击程序经常伴随着垃圾邮件,造成病毒利用邮件传递快速地蔓延,黑客程序使用户的资料意外泄漏,另外,具有欺骗性的病毒邮件,让很多企业深受其害,即便采取了很好的网络保护策略,依然很难避免,越来越多的安全事件都是因为邮件产生的。Phishing 的假冒诡计对于普通使用者来说,的确很难作出正确的判断,但是造成的损失却是很直接的,用户对网络的不信任感加重,为此公安部、教育部、信息产业部、国务院新闻办在 2004 年 2 月专门作出部署,开展互联网垃圾电子邮件专项治理工作,净化互联网环境。

人们开发了许多技术来遏制垃圾邮件的蔓延,主要可以分为四大类:过滤器(Filter)、反向查询(Reverse lookup)、挑战(Challenges)和密码术(Cryptography)。DKIM (DomainKeys Identified Mail)域密匙认证邮件技术属于反向查询技术的一种,综合了雅虎的 DomainKeys 验证技术和思科的 Internet Identified Mail 技术。DKIM 定义电子邮件的域级认证框架,利用公共密钥加密技术和关键服务器技术,使邮件传输代理或邮件用户代理可以对信件来源和内容进行验证。这种框架的目标是证明保护信件发送者的身份和他们寄出的信件的完整性,同时保持 Internet 电子邮件的功能不变。该技术标准已经提交给 IETF,得到了 Sendmail、Aol 等众多邮件服务提供商的支持。

## 2 常用的反垃圾邮件技术

### 2.1 过滤技术

过滤技术是一种最简单和最直接的技术,使用最广泛。目前市场上很多邮件服务器上的反垃圾邮件插件、反垃圾邮件网关、客户端上的反垃圾邮件功能等,都采用过滤技术。主要的过滤技术包括:关键词过滤,黑白名单,HASH 技术,基于规则的过滤,基于贝叶斯算法的过滤等。

关键词过滤技术是创建一些与垃圾邮件关联的单词表,通过邮件标题或全文的比对,来识别和处理垃圾邮件。

黑名单(Black List)和白名单(White List)。分别是已知的垃圾邮件发送者或可信任的发送者 IP 地址或者、邮件地址。现在有很多组织都在做 * bl(block list),将那些经常发送垃圾邮件的 IP 地址(甚至 IP 地址范围)收集在一起,做成 block list,比如 spamhaus 的 SBL(Spamhaus Block List),一个 BL,可以在很大范围内共享。许多 ISP 正在采用一些组织的 BL 来阻止接收垃圾邮件。白名单则与黑名单相反,对于那些信任的邮件地址或者 IP 就完全接受了。

HASH 技术是邮件系统通过创建 HASH 来描述邮件内容,比如将邮件的内容、发件人等作为参数,最后计算得出这个邮件的 HASH 来描述这个邮件。如果 HASH 相同,那么说明邮件内容、发件人等相同。这在一些 ISP 上在采用,如果

赵 毅 硕士生,主要从事计算机网络安全研究。

出现重复的 HASH 值，那么就可以怀疑是大批量发送邮件了。

基于规则的过滤根据某些特征来形成规则，通过这些规则来描述垃圾邮件，符合规则的将被过滤掉。

基于贝叶斯算法的智能过滤是使用较多的过滤方式，贝叶斯理论现在在计算机行业中应用相当广泛，这是一种对事物的不确定性描述。首先分析大量的垃圾邮件和大量的正常邮件，算法分析邮件中多种特征出现概率，形成判别垃圾邮件的规则，来过滤垃圾邮件。贝叶斯过滤器也有自适应能力，能自动进行调整。

### 2.2 反向查询技术

多数垃圾邮件工具都可以伪造邮件头，伪造发送者，或者隐藏源头。如果我们能够采用类似黑白名单一样，能够更智能地识别哪些是伪造的邮件，哪些是合法的邮件，那么就能从很大程度上解决垃圾邮件问题，验证查询技术正是基于这样的出发点而产生的，它在接受邮件的时候通过反向查询、验证邮件的真实性来确定垃圾邮件。主要有 Yahoo 和 Cisco 的 DKIM 技术，Microsoft 的 SenderID 技术，和 IBM 的 FairUCE 技术。其中 DKIM 技术实现最简便高效，得到广泛的支持，有望成为行业标准。

### 2.3 挑战技术

挑战的技术通过延缓邮件处理过程，将可以阻碍大量邮件发送者。那些只发送少量邮件的正常用户不会受到明显的影响。主要有挑战-响应技术和计算性挑战两种。

### 2.4 密码术

密码术是采用密码技术来验证邮件发送者的方案。这些系统采用证书方式来提供证明。没有适当的证书，伪造的邮件就很容易被识别出来。主要采用的技术有 AMTP，MTP，S/MIME 、PGP/MIME 几种。

## 3 DKIM 工作原理

DKIM(DomainKeys Identified Mail) 技术基于雅虎的 DomainKeys 验证技术和思科的 Internet Identified Mail。雅虎的 DomainKeys 利用公共密钥密码术验证电子邮件发件人。发送系统生成一个签名并把签名插入电子邮件标题，而接收系统利用 DNS 发布的一个公共密钥验证这个签名。思科的验证技术也利用密码术，但它把签名和电子邮件消息本身关联。发送服务器为电子邮件消息签名并把签名和用于生成签名的公共密钥插入一个新标题。而接收系统验证这个用于为电子邮件消息签名的公共密钥是授权给这个发件地址使用的。

DKIM 将把这两个验证系统整合起来。它将以和 DomainKeys 相同的方式用 DNS 发布的公共密钥验证签名，它也将利用思科的标题签名技术确保一致性。

DKIM 给邮件提供一种机制来同时验证每个域邮件发送者和消息的完整性。一旦域能被验证，就用来同邮件中的发送者地址作比较检测伪造。如果是伪造，那么可能是 spam 或者是欺骗邮件，就可以被丢弃。如果不是伪造的，并且域是已知的，可为其建立起良好的声誉，并绑定到反垃圾邮件策略系统中，也可以在服务提供商之间共享，甚至直接提供给用户。

具体的阻断垃圾邮件方式有这几种。首先，如果收到没有标记的邮件，来自那些始终用域名密钥标记邮件的域名，接受邮件的系统可以自动将其断绝或隔离，因此可以有效地阻挡垃圾邮件及诈骗邮件。第二，发件人认证系统可以建立「发件人评价数据库」，并且将此数据库公开在网络上分享给其它电子邮件提供商，其它电子邮件提供商可以参考这样的评价系统。例如，针对 www. example. com. cn 公司发送的邮件，在域名密钥的运作下，它将会有相关的数据存在「发件人评价数据库」中，而其它电子邮箱提供商将可以参考这份评价，来设定对于 www. example. com. cn 的相关规定。第三，藉由追踪发件服务器来阻挡伪造的发件人地址，通常发送垃圾邮件的人不会希望他们的发件服务器被追踪，因此他们将在域名密钥的运作下无处可躲。

DomainKeys 的实现过程如图 1 所示。

发送服务器经过两步：

①建立。域所有者需要产生一对公/私钥用于标记所有发出的邮件(允许多对密钥)，公钥在 DNS 中公开，私钥在使用 DomainKey 的邮件服务器上，如图 1 步骤 1。

②签名。当每个用户发送邮件的时候，邮件系统自动使用存储的私钥来产生签名。签名作为邮件头的一部分，然后邮件被传递到接收服务器上，如图 1 步骤 2。

接收服务器通过三步来验证签名邮件：

①准备。接收服务器从邮件头提取出签名和发送域(From:)然后从 DNS 获得相应的公钥。

②验证。接收服务器用从 DNS 获得的公钥来验证用私钥产生的签名。这保证邮件真实发送并且没有被修改过。

③传递。接收服务器使用本地策略来作出最后结果，如果域被验证了，而且其他的反垃圾邮件测试也没有决定，那么邮件就被传递到用户的收件箱中，否则，邮件可以被抛弃、隔离等。

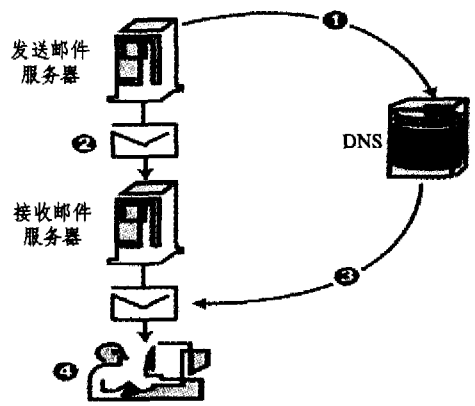


图 1 DKIM 工作原理图

对于银行、公用设施、电子邮件商务服务和其他向消费者发送交易电子邮件的公司来说，利用 DKIM 签署电子邮件的好处是巨大的。同时，DKIM 的实现也是简便高效的。首先，实施 DKIM 成本低，只需要更新现有邮件系统的配置，而不需要昂贵的专用垃圾邮件处理设备。第二，它不需要第三方认证系统，降低了成本，增强实施的可行性。第三，最终邮件用户不需要作任何的修改。

## 4 在 Sendmail 中应用 DKIM

Sendmail，Qmail，Port 25's，MDaemon MTA，StrongMail 等邮件服务系统都对 DKIM 提供支持，Sendmail 是目前应用最广泛的邮件服务系统，Sendmail 邮件服务系统从 8.13 版本

(下转第 117 页)

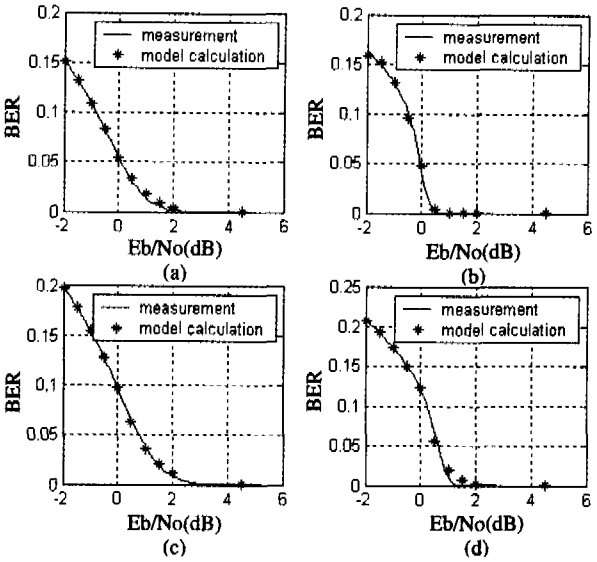


图 6 模型预测结果与实测数据比较

(a) rate = 1/3, length = 64; (b) rate = 1/3, length = 1024; (c) rate = 1/2, length = 64; (d) rate = 1/2, length = 1024

模型参数，通过简单的计算，可以预测出在一定码率、交织长度及信道信噪比条件下系统的误比特率。实验证明，该模型可以精确地与实测结果相吻合。利用该模型，可以在发送端"掌握"原本只能在解码端得到的误比特率，从而可以指导信源信道联合编码中的码率分配并应用在端到端的率失真优化中。

如何在不过多增加模型复杂度的基础上考虑更多的参数的影响，以及如何将模型延伸到信源编解码部分，是需要进一步研究的方向；其次，尽管该模型是简单并且有效的，但是仍然需要从理论上推导出一个具有类似复杂度且精确实用的模型，并给出理论上的解释。

## 参 考 文 献


1 Berrou C, Glavieux A, Thitimajshima P. Near Shannon Limit Error-correcting Coding and Decoding: Turbo-Codes. In: Proc. ICC'93, Geneva, Switzerland, 1993(5): 1064～1070

2 GPP2 C. S0002-A Version 55: Physical layer Standard for cdma2000 Spread Spectrum Systems Release A, 1999.12

3 TS25.212 V2.2.0(1999-09) 3GPP ; Technical Specification Group; Radio Access Network

4 Ma X F, Lynch, W E. Iterative joint source-channel decoding using turbo codes for MPEG-4 video transmission. Acoustics, Speech, and Signal Processing, Proceedings (ICASSP '04), IEEE International Conference on, 2004, 4: 657～660

5 刘东华. Turbo码原理与应用技术. 北京：电子工业出版社，2003

6 Benedetto S, Montorsi G. Unveiling Turbo-codes: Some results on parallel concatenated coding schemes. IEEE Transactions on Information Theory, 1996, 42(2): 409～429


(上接第 91 页)

开始支持 DKIM，通过 Sendmail Milter(mail filter API)实现，安装 Milter 之前，系统必须安装 OpenSSL 库文件，在域名服务器中修改 DNS 记录，并安装有 Sendmail 8.13 版本以上的服务程序，下面介绍在 Sendmail 中 DKIM 的具体配置和实现。

①安装 DKIM Milter

- 在 Sendmail.net 上下载 DKIM Milter 源程序并解压
- 按照配置说明编辑 dkim-filter/Makefile.m4 文件
- 改变当前目录为解压文件目录，并执行下列命令：sh Build
- 如果没有任何错误，执行下面的命令安装程序：sh Build install

②生成公有密匙和私有密匙

- 键入以下命令产生私有密匙：openssl genrsa -out rsa.private 768
- 键入以下命令产生公有密匙：openssl rsa -in rsa.private -out rsa.public -pubout -outform PEM
- 移动私有密匙到 domainkeys 目录，并改为相应的名字：mv rsa.private /var/db/domainkeys/mail.key.pem

③生成 DNS TXT 记录

建立一个例如 selector._domainkey.example.com 的 DNS TXT 记录如下：

mail._domainkey.example.com. IN TXT "g=; k=rsa; t=y; p = MEwwPQRJKoZIhvcNADAQCQADOwAwOAIxANPpYHdE2tevfEpvL1Tk2dDYv0pF28/f5MxU83x/0bsn4R4p7waPaz1IbOGs/6bm5QIDAQAB"

p=后面的字串是基于 base64 编码的公有密匙，t=y 表示是测试模式

④启动 DKIM Milter

Milter 程序作为后台程序运行，如果你以超级用户运行 Milter，必须建立一个非特权用户，比如建立一个名称为 DKIM 的用户，使用下面的命令启动 Milter：

/usr/bin/dkim-filter -l -p inet:8891@localhost -c nowsp -d example.com -s /var/db/dkim/mail.key.pem -S mail -u dkim -m MSA

⑤按照 DKIM Milter 重新配置 sendmail.cf，重建后重新启动 Sendmail

⑥测试 DKIM

为了确定 DKIM 是否配置正确，可以发送邮件到 autorespond+dkim@dk.elandsys.com 进行验证，下面是一个经过签名的邮件头的范例：

DKIM-Signature: a=rsa-sha1; c=nowsp; d=example.com; s=mail; t=1121360586; h=Received:Date:Message-Id:From:To:Subject; b=c+whUn73dM6nvFUMLTzCug-4IbskDZtKpv9FFk1DACg9zTADH60+2nIyuZCZwlPiL

如果配置成功，你可以在你的邮件头中发现下面的信息：

Authentication-Results: mail.example.net; dkim=pass

**结束语** DKIM 作为一种新的反垃圾邮件技术标准，已正式提交 IETF，有望成为行业标准。该标准得到大多数邮件服务厂商的支持，并具有高效、部署容易、成本低等优点，将成为反垃圾邮件的主流技术。

## 参 考 文 献


1 http://mipassoc.org/dkim/index.html

2 http://antispam.yahoo.com

3 http://www.identifiedmail.com/

4 http://www.sendmail.net/

5 http://www.ietf.org/internet-drafts/draft-allman-dkim-base-01.txt

6 http://www.ietf.org/internet-drafts/draft-allman-dkim-ssp-01.txt

7 Refdom. 反垃圾邮件技术解析. http://www.xfocus.net/releases/200508/a818.html

8 http://domainkeys.sourceforge.net/