基于 Qmail 的邮件安全策略①

苏宝莉，谭 鹏

(常州机电职业技术学院，常州 213164)

摘 要：首先通过危害性邮件对本单位所造成的影响，分析使用的中 Qmail 邮件系统存在的安全问题，并对可设置的安全策略进行研究，通过对邮件系统安全策略的实际改进，提高本单位邮件系统对危害性邮件的抵御能力，以保证使用者的邮件安全。文中主要对当前较为普遍的邮件安全策略进行分析研究，针对我单位的实际情况，通过设置合适的邮件安全策略，提高本单位的邮件安全性。

关键词： qmail；垃圾邮件；安全；策略

E-Mail Security Strategy of Qmail

SU Bao-Li, TAN Peng

(Yunnan Academy of Scientific & Technical Information, Kunming 650051, China)

Abstract: This article, first by e-mail on the harmful impact of the unit, analyzes the Qmail mail system used by security problems, and can set the security policy studies, through the mail system security policy on the actual improvements to enhance the message of this unit System resilience of the harmful messages to ensure the safety of users e-mail. In the main text of the current of the more common e-mail security policy analysis and research unit for my actual e-mail by setting appropriate security policies, improve the unit's e-mail security.

Keywords: qmail; spam; security; strategy

电子邮件系统是一种用电子手段提供信息交换的通信方式。是 Internet 应用最广的服务，通过网络的电子邮件系统，用户可以用非常低的成本，以非常快速的方式，与世界上任何一个角落的互联网用户联系，这些电子邮件可以是文字、图像、声音等多种媒体格式。同时，通过电子邮件用户可以订阅大量免费的新闻、专题邮件，并实现轻松的信息搜索。

Qmail 是基于 UNIX 操作系统的 Internet 邮件传输机构(Internet Mail Transfer Agent 简称 MTA)。它采用标准的简单邮件传输协议 SMTP 与 Internet 上其他邮件传输代理 MTA 交换信息。Qmail 提出了 Maildir 存储方式，每个邮件作为单独的一个文件保存在用户个人的邮件目录下，这就避免了加锁。同时，Qmail 支持虚拟域(Virtual Domain)和虚拟用户(Virtual User)，使邮件系统的用户独立于 UNIX 系统用户。Qmail 的 MTA 依然是世界上转发速度最快的邮件传输代理，Qmail 几乎兼容所有的 Linux/Unix 类操作系统。基于 Qmail 的一系列优点，我单位在建立自己的邮件系统之初就就选用了 Qmail 邮件系统加 Linux 系统平台的单位邮件系统解决方案。使用中极大地便利了人员的信息交流，提高了工作效率。但随着近年来危害性邮件的泛滥，据 Pingdom 公司公布的统计数据[1]：全球网民总量(截至 2009 年 9 月)：17.3 亿，2009 年全球电子邮件发送量：90 万亿，垃圾邮件比例：81%，垃圾邮件年末峰值比例：92%，垃圾邮件同比增幅：24%，垃圾邮件日均发送量(按照 81%计算)：2000 亿；面对如此严重的垃圾邮件问题，Qmail 的原有架构体系无法有效处理。Qmail 的整体模块主要由 MTA、MDA、MUA 三大部分组成，而 Qmail 的 MTA 和 MDA 中没有任何对邮件的检测和过滤的措施。垃圾邮件不仅占据并浪费了宝贵的网络资源，而且带来了严重的社会问题。因为垃圾邮件，有些 IP 地址被反垃圾邮件组织和网络运营商列入了黑名单，严重影响了网络的正常使用。破坏了电子邮件的正常流通秩序，对单位的正常信息

① 收稿时间:2010-05-14;收到修改稿时间:2010-07-05

通信的危害十分严重。针对一系列问题，通过对 Qmail 邮件系统邮件收发机理的研究，发现 Qmail 存在的缺陷，深入探究邮件安全机制，对比不同安全策略的优缺点，完善本单位的 Qmail 邮件系统。防止垃圾邮件对本单位工作的干扰与破坏。

1　Qmail邮件系统的安全问题

Qmail 为本单位提供了便利的电子邮件服务。Qmail 的整体模块主要由 MTA、MDA、MUA 三大部分组成。如图 1 所示：

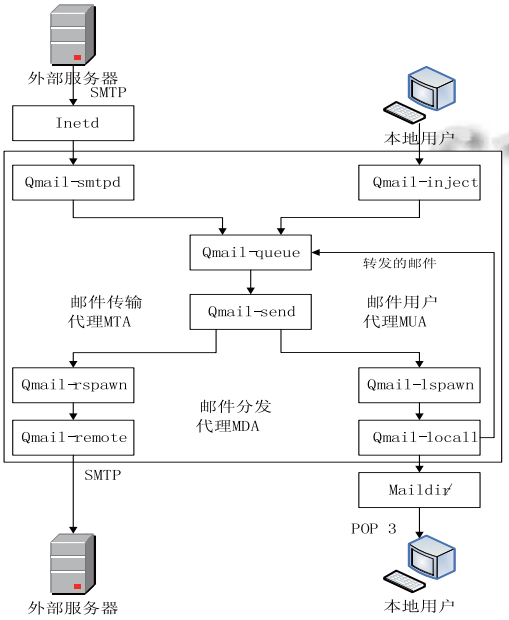

图 1　Qmail 系统结构图

对于一个基于模块化设计的邮件系统，它的每一个子功能都是由一个进程实现，而每个进程的属性以及运行方式则由一个或多个配置文件和环境变量来控制。默认配置中，Qmail 的 MTA 和 MDA 中基本没有对邮件的检测和过滤措施，这无疑成为邮件用户的一种安全威胁。

1.1 Qmail 存在的问题

根据对本单位邮件服务器的(什么方法)检查，发现邮件服务器处于开放式中继(Open-Relay)状态，需要设置 SMTP 认证；没有安装基于 Linux 系统平台下的 Qmail 邮件系统杀毒软件；没有设置有效地邮件过滤机制。

1.1.1 Open-Relay 产生的问题

Open-Relay 是指邮件服务器不需验证邮件发送者或邮件接受者的是否为系统所设定的用户，而对所有的入站邮件一律进行转发[2]。Qmail 在缺省状态下不支持对 Smtp 用户的认证，导致任何能访问该 Qmail 服务器的用户均可以利用此邮件服务器来向任何地址发送邮件。本单位之前曾多次被列入邮件黑名单，导致主要邮件服务商拒绝接收本单位邮件，主要就是由于邮件系统处于开放式中继状态；因此，首先需要关闭 Open-Relay 功能。

1.1.2 邮件病毒

恶意垃圾邮件即病毒邮件，邮件携带了病毒体，一般通过附件来携带病毒文件。过滤该类恶意垃圾邮件，需要具备病毒查杀功能，这就要求我们安装基于 Linux 系统的杀毒软件。

1.2 垃圾邮件分层过滤

垃圾邮件的过滤是防范垃圾邮件重要的安全措施之一。垃圾邮件的过滤可以基于 IP 地址，邮件的信头或者邮件的内容，可以在邮件用户、MUA、MDA、MTA、网关、路由器、防火墙等多个层次进行[3]。各层次情况如图 2 所示：

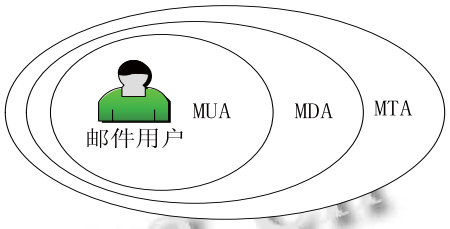

图 2　垃圾邮件过滤层次图

1.2.1 MTA 过滤

相对于现在的网络环境，在本单位使用 Qmail 邮件系统之时，垃圾邮件问题并不突出，Qmail 的配置文件基本都是默认配置，现需对配置文件进行重新配置，并对一些漏洞进行补丁修补。

1.2.2 MDA 过滤

邮件投递代理层的过滤主要是针对邮件内容的过滤，可以设置黑白名单、自动分类和处理等功能。能够根据要求对邮件头和邮件体的内容进行过滤，防止通过电子邮件传播病毒、通过邮件对系统的恶意攻击、阻挡广告类的垃圾邮件，还可以帮助管理用户所接收的邮件。所以 MDA 层的过滤显得尤为重要。

1.2.3 MUA 过滤

邮件用户代理 MUA 则基于客户端，也有基于 Web

方式的。本单位的邮件用户一般均采用 Windows 下的 Outlook，而 Outlook 支持 MUA 过滤。

2 解决问题

2.1 关闭 Open-relay

由于本单位使用的 Qmail 邮件系统主要是对本单位局域网用户提供邮件服务，可将邮件系统设置为非 Open-relay 模式，使用 ucspi-tcp 软件包中的 tcpserver 程序，修改 tcp.smtp 配置文件以使邮件系统只对本单位局域网用户进行邮件转发。具体配置如下：

127.0.0.1:allow，RELAYCLIENT=""

192.168.*.*: allow，RELAYCLIENT=""

:allow

其中，192.168.*.*为本地网络地址为 192.168.*.0/24 的 C 类地址。通过此设置，保证了只有本地用户可以转发邮件，防止了邮件转发被滥用。

2.2 检查 Qmail 配置文件

Qmail 的配置文件是由多个文件组成，每个文件控制相应部分的功能和属性，一个可执行程序可能有多个配置文件控制,所有的配置文件共同决定了 Qmail 运行的实现和模式。对于 concurrencylocal、concurrencyremote、me、queuelifetime 等文件保持默认状态不变。

修改 databyes 文件，设定 qmail-smtpd 所允许接收邮件的最大字节数为 10 兆。具体修改如下：

echo 10485760 > /var/qmail/control/databyts

2.3 安装杀毒软件

安装 Clamav 免费杀毒软件[4]，实现对进入邮件队列的邮件杀毒。首先，创建杀毒软件用户，useradd –s /bin/false clamav；并安装 Clamav。配置 clamd.conf 杀毒配置文件，在 Example 前加#；配置 freshclam.conf 升级配置文件，在 Example 前面加#，并将 Checks 的值修改为“8”，即每 8 小时更新一次病毒码；然后启动杀毒软件。

2.4 对邮件安全策略的完善

原本的 Qmail 由于使用的时间较早，基本没有考虑到邮件安全问题，通过对完善现有安全策略可以做到对大部分垃圾邮件的过滤。主要为邮件内容过滤，邮件队列扫描和第三方 RBL 服务的引入。

2.4.1 邮件内容过滤

安装 Spamassassin 的 rpm 包，并配置启动脚本使其支持 vpopmail。修改过滤模板文件 local.cf 定义邮件评分线为 7.0，如果超过平行线将在邮件标题开头处加入“****SPAM****”字样，提示为垃圾邮件。使用 CCERT 中文垃圾邮件过滤规则集 Chinese_rules.cf：

Wget –N –P /usr/share/spamassassin www.ccert.edu.cn/spam/sa/Chinese_rules.cf

2.4.2 邮件队列扫描

安装邮件队列扫描程序，具体安装设置如下：

./configure --qmail-queue-binary /var/qmail/bin/qmail-queue

--setuidgid-path /usr/local/bin/setuidgid – admin ***

--domain?***.net.cn

--notify sender,admin

--local-domains?***.net.cn --lang en_GB --debug yes --unzip yes --scanners clamscan,fast_spamassassin --virus-to-delete yes --sa-forward ***@***.net.cn --sa-reject yes --sa-subject "*** SPAM *** "

其中“***”为本单位所涉及的邮件账户名及邮件域名。

安装结束后，先检查 qmail-scanner-queue.pl 文件存在，然后修改 vpopmail 的配置文件，添加：

127.0.0.1:allow,RELAYCLIENT="",RBLSMTPD="",QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"。

修改 qmail-scanner-queue.pl 文件内容：

my $clamscan_options= " -r – mbox --disable-summary – max-recursion=10 – max-space=100000”。

Maildrop

2.4.3 第三方的 RBL 服务

RBL(Realtime Blackhole List)是实时黑洞列表[5]，国际上的反垃圾邮件组织(如 MAPS、ORBS、SpamCop 等)都提供 IP 地址数据库(或黑名单)。垃圾邮件地址黑名单以 DNS 记录的形式存储在 DNS 服务器中，可以配置邮件服务器订阅 RBL 的黑名单，邮件服务器在收到 SMTP 的请求后用源发的 IP 地址实时检索 RBL，如果该 IP 地址在 RBL 黑名单中则拒绝接收。

Qmail 的 rblsmtpd 必须和 ucspi-tcp 结合在一起使用，而在 ucspi-tcp0.88 版本中已经包含了 rblsmtpd，所以在此不需单独下载安装 rblsmtpd。修改 SMTP 启动脚本，增加第三方 RBL 列表根据本单位实际情况，

RBL 引用的为“中国反垃圾邮件联盟”推出的 CASA RBL。具体配置如下：

```
/usr/local/bin/tcpserver -H -R -l 0 -t 1 -v -p -x \
 /home/vpopmail/etc/tcp.smtp.cdb -u qmaild -g nofiles 0 \
smtp /usr/local/bin/rblsmtpd \
-r cbl.anti-spam.org.cn \
-r relays.ordb.org \
/var/qmail/bin/qmail-smtpd your.host.name \
/home/vpopmail/bin/vchkpw /bin/true 2>&1 | \
/var/qmail/bin/splogger smtpd 3 &
```

3 邮件安全策略检查

通过上一节对邮件系统的安全策略设置，分别验证其有效性，具体结果如下。

3.1 测试杀毒软件

运行：# clamdscan －邮件目录

参数：－o(对从系统向外发送的邮件做过滤)

参数：－l(对发到系统的邮件做过滤)

在扫描病毒时设置—remove 参数，可同时删除病毒文件，通过以下的杀毒状态图，可以肯定 Clamav 杀毒软件是有效可行的。

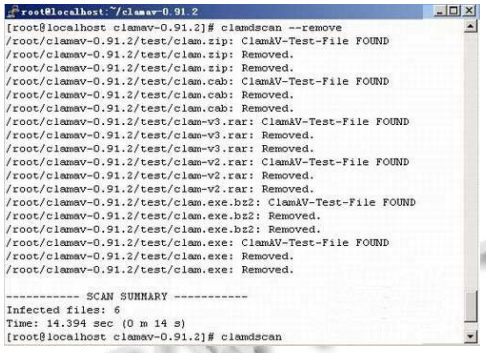

图 3　Clamav 杀毒软件杀毒状态图

3.2 病毒邮件测试

通过发送一封带有病毒附件的测试邮件到指定邮件账号，查看 tail -f/var/spool/qscan/qmail-queue.log ，可以看到病毒邮件被扫描发现，并被删除。可在 quarantine.log 日志文件中查看记录。

3.3 垃圾邮件测试

通过发送一封带有需过滤词汇的测试邮件到指定邮件账号，同样查看 tail -f/var/spool/qscan/qmail-queue.log，发现邮件经过评分，且评分超过 7.0，接收到的垃圾邮件标题开头加入了 SPAM 字样。通过查看邮件属性，也确定了邮件经过处理的记录。

3.4 黑名单测试

本单位原来也设置过第三方 RBL 服务，但是效果一般，原因在于，所接收的大量垃圾邮件为国内发出的中文垃圾邮件。所以采用 CASA RBL 服务，CBL 主要面向中国国内的垃圾邮件情况，所甄选的黑名单地址也以国内的垃圾邮件反馈情况为主。可以说，CBL 比国外的一些 RBL 服务器更适合中国国情。

4 结论

邮件过滤是邮件安全策略的重要部分，在实际应用中很难通过简单的现有方式做到完全的邮件过滤，必须采用多种手段结合的方式，建立多层次的安全体系，才可有效减少垃圾邮件数量。通过对本单位 Qmail 邮件系统的安全策略更新，阻止了相当数量的垃圾邮件，然而防范垃圾邮件最根本的因素还是人，需要培训邮件使用者，使邮件使用者知道为什么要防止垃圾邮件，必须做些什么。垃圾邮件之所以能够被发送，有部分原因就是最终用户不重视也不知道如何防范垃圾邮件。

参考文献

1 Pingdom. Internet 2009 in number. [2010-1-22]. http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/

2 李崴. 基于 qmail 的反垃圾邮件系统构建.黄石教育学院学报,2004,(12):72－75.

3 段海新.防范垃圾邮件技术.中国计算机用户,2004(2):27－27.

4 华江.为 Linux 各种应用服务器配置 Clamav 防毒工具 it168, 2008,(7):30.

5 张波,吴开超.反垃圾邮件原理和技术初探.中国科学院科学数据库.[2007-10-23].http://www1.csdb.cn/ prohtml/0.fruits.papers/pages/0200.html