PRL TN-2006-86

PRL Technical Note

Management of Email From Risks and Threats At PRL

Jigar Raval
Computer Centre

June 2006

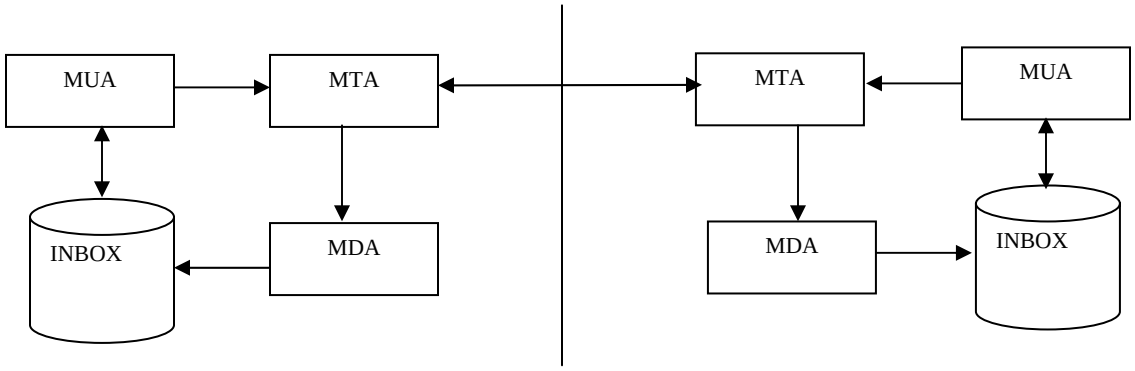
Physical Research Laboratory
Navrangpura, Ahmedabad-380 009

Contents

1. INTRODUCTION

The beginning of Internet connectivity on PRL desktops can be traced to the introduction of E-mail facility first configured around 1988-1989 on a Nexas-Appolo 3500 machine. At that time UUCP (Unix to Unix Communication Protocol) on a telephone dial-up lines of 9.6Kbps under Sys-V (Unix) operating system was made operational. This facility was extensively used in PRL. In order to reduce operating costs, scripts were written for auto dialing during late night hours to the NCST gateway, Bombay, for sending and receiving the e-mails. As at that time there was no Local Area Network (LAN) in PRL physical transfer of mails from and to PRL mail server machine using external media was common. This scenario changed drastically in 1993 after installation of IBM RS-6000/580 machines with 10Mbps LAN. Simultaneously, PRL subscribed to DOE-ERNET using VSAT hub at Bangalore. All these developments brought about dramatic changes in functionality and e-mail, File Transfer Protocol (ftp) etc. became available on individuals desktops.

The dramatic growth of Internet and communication systems over the past decade has created a remarkable and radical change in the way individuals communicate and businesses operate. Electronic mail has become one of the most influential technologies. It is also a critical medium for sharing information within an organization as well as between different organizations. Fig.1 shows basic functionality of a typical email system.



MTA – Mail Transfer Agent
MDA – Mail Delivery Agent
MUA – Mail User Agent

Fig. 1

While email has greatly increased the efficiency in information communication, risks and threats associated with email has also increased substantially. Specifically, external threats like viruses and spam mails jeopardize the security of an organization's electronic infrastructure. Two of the top trends highlighted by the Computer Emergency Response Team (CERT) are that attacks are increasing in sophistication and in automation. System

vulnerability is best dealt with proactively because, often, it is too late to respond once viruses get into the network.

There are many anti-spam and anti-virus tools available. Some are available as open source (free) and others are commercial tools which are required to be purchased. *SpamAssassian* is an open-source free anti-spam tool. It encompasses many of the current anti-spam techniques in a single package; moreover it is easy, flexible and highly configurable. New techniques to identify spam, such Sender Policy Framework (SPF), Spam URI RealTime Blocklists (SURBL) etc. can be added by developing them as modules. These modules are configurable, customizable and scalable to large architectures. *Clamav* is also an open-source anti-virus tool. It is easy to install and configure. In this technical report we shall discuss various risks and threats that are associated with email and both the above mentioned tools are deployed to manage email risks and threats.

2. Email Risks and Threats

2.1 SPAM:

Spam is unsolicited commercial email, usually junk mail. Spam is very common and often frustrating. Sometimes it floods the mail server with lots of junk mail. It thus causes loss of productivity and utilizes bandwidth. Therefore, every organization must take appropriate measures in order to block spam from entering their email system. Spam distribution method, spam characteristics, and anti-spam techniques will be discussed in this report.

In order to effectively filter out spam and junk mail, we need to be able to distinguish spam from a genuine mail. To do this, we need to identify typical spam characteristics, and various spam distribution methods that are used to generate spam mail.

2.1.1 Spam Distribution Methods:

There are many ways of spamming. The commonly used ones are:

(a) Open Relay (b) Open Proxy Server
(c) On-the fly spammers

(a) Open Relay:

In the open relay method an email server permits a third party to relay email messages where neither the sender nor the recipient is a local user. Fig. 2.1.1 displays the functioning of an open relay server.

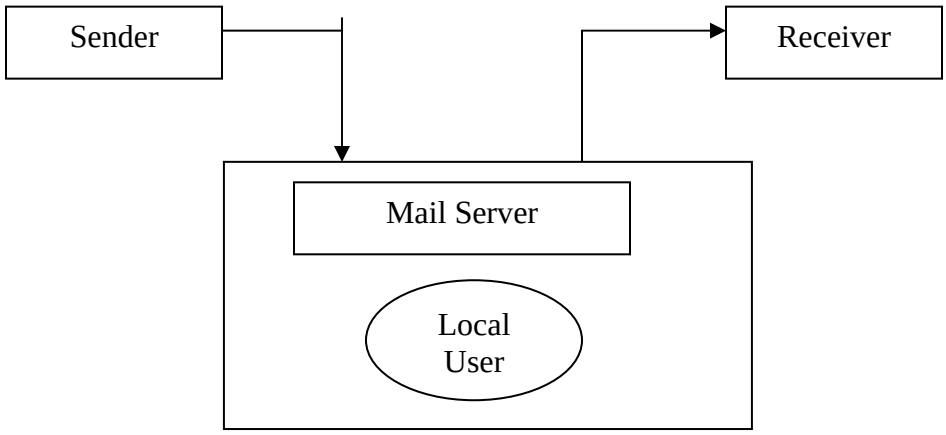


Fig. 2.1.1

Spammers find out this type of system on Internet. By relaying mail through open relay mail servers they flood the Internet with large amount of junk mail in a very short period of time.

Following are the consequences:

- Mail system of the organization that suffers from open relay may crash and might possibly lose important data.
- The worst consequences are that organizations /companies that are open relay will often be blacklisted by other organizations and overall result is the loss of credibility. Therefore, care should be taken while setting up a mail server to ensure that unauthorized relaying is not permitted.

Appendix I shows examples of *postfix* and *qmail* configuration file to disable open relay system.

(b) Open Proxy server:

A proxy server is simply a system that takes an Internet request, such as web server connection request from, a computer and forwards it to another computer as if it had originated locally from that host. If proxy server is configured to accept requests from anyone, without any form of prior authentication, it is known as an Open Proxy. Open Proxies are far more serious than open relay. Various blacklists exist that will block connection from systems connected via open proxies.

How the server can be configured not be Open Proxy:

First, always deny any requests that does not come from the local network i.e. “deny all, allow specific”. For example,

```
Acl mynet src 192.168.1.0/16
http_access allow mynet
http_access deny all
```

Second, to add additional security, one should make sure that squid never connects to another server’s SMTP port:

```
Acl SMTP_PORT port 25
http_access deny SMTP_PORT
```

In fact, there are many well-known TCP ports, in addition to SMTP to which squid should never connect to.

(c) On the fly spammer:

Free mail services like “yahoo” and “hotmail” have revolutionized access to the Internet for many people, but unfortunately they have also become a major source of spam. It is very easy to open an account in this type of services by spammers. Many spammers have developed automated tools that would perform account creation and spam delivery automatically. It is important to note that 70% of all spam appears to originate from one of the major free mail services; in reality a significant proportion of the addresses used are fake and are not real. This is why non-deliverable spam with free mail addresses almost always comes back with “user unknown” message.

In recent times, most of the free mail services have tightened their security system significantly and it is now more difficult for spammers to use these services. For example, “yahoo” and “gmail” have implemented a *“domain keys”* concept.

2.1.2 How to effectively block spam mail:

In order to effectively filter out spam mail, we need to be able to distinguish spam from genuine messages. Normally, spam characteristics appear in two parts of a message (1) email headers and (2) email message content.

(a) Email Header :

Email headers contain information about the sender and recipient, date and time of transmission, subject, the route an email has taken in order to arrive at its destination, besides other information. Most spammers try to hide their identity by forging email headers or by relaying mail to hide the real source of message. Here we shall discuss how to distinguish a spam message from a genuine message by looking at the mail headers.

In brief, following characteristics are normally observed in spam messages:

- Recipient’s mail address is not in the To: or Cc: fields
- From: field is the same as To: field
- Missing From: field – to disguise the actual sender of message
- Code and space sequence exist
- Illegal HTML exists
- To: field is empty
- X-UIDL header exists

(b) Message Contents:

Apart from email headers, spammers tend to use certain word/language in their emails that organization can use to distinguish spam messages from legitimate messages. Typical words are *free, online casino, limited offer, earn money, viagra, need your assistance, urgent and confidential* and sometimes over use of capitals in the text. Checking words in the email body and subject can block it, but it is important to filter words accurately. **Appendix III** shows *SpamAssassin*[4], an anti-spam technology to block spam mail based on message content.

2.1.3 Anti-spam technology:

With the knowledge of typical spam characteristics and spam distribution methods. There are various solutions available but here only those which are freely available on Internet are discussed. These are easy to configure with MTAs like qmail and postfix.

(a) Block spam by checking IP / domain in Real time Blackhole Lists (RBLs):

There are various non-profit organizations who maintain databases that contain IP addresses and domains of known spammers. For example, open relay database (ORDB), Spamhaus Block List (SBL) etc. By using these databases a large amount of spam can be filtered out showing configuration file of qmail and postfix to use RBL. RBLs are effective technique for blocking spam. With careful selection of RBL, one can effectively eliminate spam. **Appendix II** shows how to use this technique in postfix and qmail.

(b) Filter out spam mail based on email header characteristics:

Email header characteristics mentioned above can safely be used to classify a mail as spam. Since checking email header is a fast process it is good to check before checking the message content.

(c) Identify message content:

There is also a possibility of spam message that gets through both filters mentioned above. The way to filter these mails is by checking the message content. For instance, messages that contain words such as online casino, viagra, are almost 100% certain of being spam. There are words that could possibly be used in genuine mails as well, such as accept credit card, need your assistance. Therefore, it is important to perform different actions on different sets of words/phrases. A better way is by giving certain words a score and then specifying score threshold per email. This procedure will decrease the amount of false positive. It is also important to apply case sensitivity criteria to the text of the message, since spammers often change the case of words/phrases case.
Appendix III shows how to use both the above techniques using *SpamAssassin*

(d) Reverse DNS lookup and DNS MX record lookup :

This is an effective spam blocking technique that uses a reverse DNS lookup on the incoming e-mail's source IP address. If the domain provided by the reverse lookup matches the from address on the email, the email is accepted. Spammers use fake addresses so that spam cannot be traced back. To determine whether a "from" address is valid or not, the system does a lookup on the domain that is used in the "from" address. If the domain does not have a valid DNS MX record, then from address is not valid and the email is labeled as spam. There are some websites which provide facility to check the MX record lookup and reverse DNS lookup facility for any domain.

There are various new anti-spam techniques available in the market. These techniques improve upon the reverse DNS lookup technique. Some are discussed below briefly.

(1) Sender Policy Framework (SPF):

Spoofing an email address is the unauthorized use of someone else's email address. It is one of the primary methods of spreading spam and viruses. SPF is an open standard security protocol designed to detect spoof email address. It checks email address against a list of all computers authorized to send email as that email address. Appropriate action can be taken based on the configuration and result. This can be configured on all the major well known MTAs like sendmail, qmail[2], postfix[3] Postfix V2.1 and above has in-built policy server. For further detail visit the following web pages

SPF --- http://spf.pobox.com/downloads.html
Postfix and SPF --- http://www.postfix.org/SMTPD_POLICY_README.html

Appendix IV shows an example of postfix configuration with policy server.

(2) Domain keys:

This is introduced by "Yahoo". The idea is to sign and verify mails at gateway level, using a public key found in DNS for verification. For more details, visit yahoo page (http://antispam.yahoo.com/domainkeys).

(3) Sender ID:

This technique is jointly developed by "Microsoft" and industry partners to stop unauthorized use of email address. For more details, visit http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx.

Users are requested to check the documentation thoroughly before using any of the above techniques.

(e) User Training :

Users must know that spam should be deleted straight away and inform their system administrator who will update the anti-spam tool. One important guideline is to never reply to spam mail as this will just confirm that the recipient's email address is active and available for further abuse. Also links in spam message should not be followed, because unwanted messages that offer an "unsubscribe" option are particularly tempting but this is often just a way for collecting valid addresses that are then used for sending spam mails.

2.2 Viruses / Worms / Trojans:

The common thing in the world of internet is email viruses. We are aware about the havoc created by "CodeRed" (July 2001), "Nimda worm" (September 2001), "Slammer worm" (January 2003), variant of "Netsky" etc. An effective anti-virus product requirement on a mail server is that it can scan all the inbound and outbound mail and then deliver virus free mail to user's mailbox. There are various commercial and open source solutions available in the market. However, based on the following common criteria one can select a good product.

- Pricing / License policy
  - Per User / mailbox
  - Per domain
  - Unlimited
- Support for MTAs
- Ease of administration
- Stability
- Performance (CPU usage)
- Time to create signatures when a new virus comes out

Among all the products, *Clamav* is an open source product with unlimited license usage. It supports for all the well-known MTAs. Following are the features of *Clamav:*

- Licensed under the GNU GPL version 2
- Posix compliant portable
- Fast scanning
- Advanced database updater with support for digital signatures and DNS based database version queries.
- Scans within Archives and compressed files, built-in support includes Zip, RAR, TAR, GZIP, MS OLE2 etc.
- Supporting on all popular operating systems like Linux, Solaris, AIX, MAC OS X etc.

Add-ons plugin required to integrate antivirus software with MTAs. Commercial as well Open source add-ons are available. For example, "**Kaspersky Lab"** includes qmail support for their antivirus program, "**Amavis", "F-prot",qmail-scanner, Mail scanner**. Among them open source solutions, like qmail-scanner is an add-on for qmail to integrate *clamav*, mail scanner for postfix. These are typically used for antivirus protection function in conjunction with external virus scanners and scan not only locally sent / received mails but also emails that passe through the server purely in a relay mode. They can also be integrated with *SpamAssassin* to block spam mails. **Appendix-V** gives examples of qmail-scanner and mail scanner configuration for qmail and postfix.

2.3 Mail Services AT PRL:

PRL mail server is configured with open source MTAs, anti-spam and anti-virus softwares. The primary mail server is configured with qmail, secondary one with postfix. Both the mail servers are on DMZ and act as an MTA. It delivers mails on a machine, which is on private local network, running sendmail. *SpamAssassian* is configured to check spam mails and *Clamav* is configured to scan the mail to protect against virus. Figure 2.3.1 shows how the PRL mail server scans incoming mails.

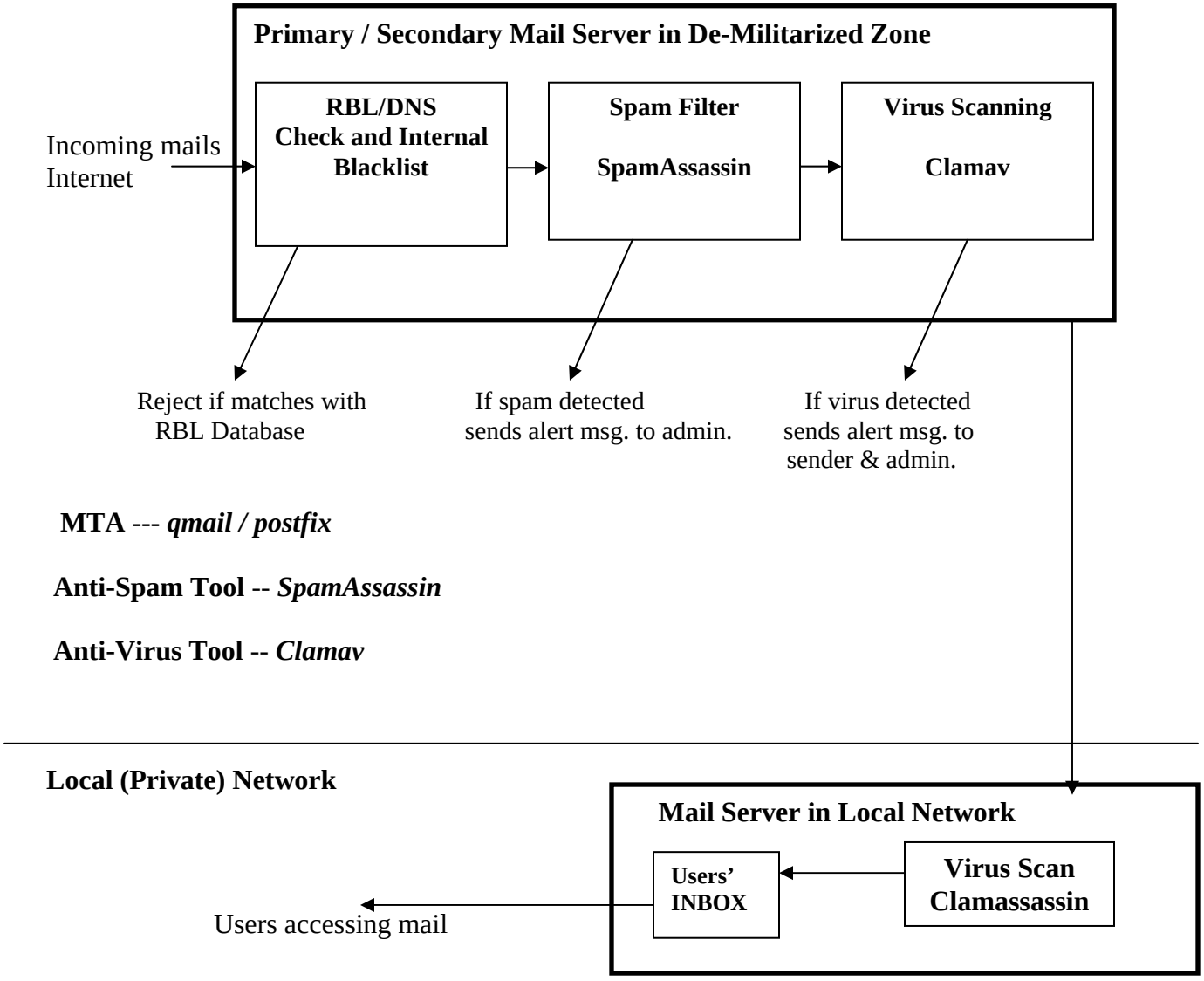


Fig.2.3.1 A schematic diagram of PRL Mail System

Techniques for spam and virus filtering have become very sophisticated and need careful implementation keeping in mind the institution policy. Although PRL uses all the above software, several implementation specific changes have been carried out by us.

(1) Keyword Filter

(2) DNS/RBL Test

(3) Header Test

(4) Message content

(5) URL Recognition

(6) Sender Policy Framework (Currently, implemented on secondary mail server)

(7) Block specific file type

As mentioned above, the mail servers at PRL act as relay server. The machine on which the users' mailbox resides is configured with Sendmail as MDA and *Clamassassin* to protect against viruses / Trojans / Worms / HTML-phishing.

To fight against spam, we have created an email account – "spam-help@prl.res.in". Users forward the suspected spam mail to this account. We analyze the reported mail with various attributes like header, message content and accordingly define the criterion with appropriate score. With overwhelming response from users, incoming spam mail reduces substantially. Almost 85% mails rejected by using RBL and from the remaining mails 30-35% mails are filtered out and classified as spam by *SpamAssassin*. **Appendix VI** and **Appendix VII** show the sample statistics of RBL and *SpamAssassin* for the month of December 2005. Similar statistics are also observed in past. As discussed, Spammers use a variety of techniques and are also continuously modifying their techniques. So there is a continuous evolution in the techniques used on both sides. We update our anti-spam technique on daily basis to effectively block spam mail.

Following is the brief information of Hardware and Software employed in PRL mail servers

(1) Primary Mail Server :

Hardware: P-IV 2.6GHz
256MB DDR SDRAM
40GB HDD
10/100/1000 Mbps NIC

Software: Operating System: *Fedora core1*

MTA : qmail

Anti-Spam Tool : *SpamAssassin*

Anti-Virus Tool : *Clamav*

Web based URL: http://mail.prl.res.in

(2) Secondary Mail Server :

Hardware: P-IV 2.6GHz
256MB DDR SDRAM
40GB HDD
10/100/1000 Mbps NIC

Software: Operating System: *Fedora Core1*
MTA : *Postfix*
Anti-Spam Tool : *SpamAssassin*
Anti-Virus Tool : *Clamav*

Web based URL: http://ppp.prl.res.in

APPENDIX-I

Stop Open Relay

Postfix:

Edit the /etc/postfix/main.cf file and include the lines:

smtpd_client_restrictions = permit_mynetworks, reject
smtpd_recipient_restrictions = permit_mynetworks, reject_unknown_client
smtpd_sender_restrictions = permit_mynetworks, reject_unknown_sender_domain

For further detail visit postfix UCE page: http://www.postfix.org/uce.html

Qmail:

Edit the /var/qmail/control/rcpthosts file to include all authorized domains like :

yourdomain.com
yourdomain1.com

Qmail also supports SMTP access control using tcp.smtp. Allow local hosts to inject mail via. SMTP

```
echo 172.16.5.:allow,RELAYCLIENT="" >> /etc/tcp.smtp
qmailctl cdb
```

Sample tcp.smtp file :

```
172.16.5.:allow,RELAYCLIENT=""
:allow
```

APPENDIX-II

Real Time Blackhole List:

Postfix RBL example configuration:

Edit /etc/postfix/main.cf file and add the lines

smtpd_client_restrictions = permit_mynetworks, reject_rbl_client relays.ordb.org

smtpd_sender_restrictions=permit_mynetworks,reject_unknown_sender_domain,
reject_non_fqdn_sender,
reject_rbl_client relays.ordb.org

maps_rbl_domains = relays.ordb.org, relays.mail-abuse.org

qmail RBL example configuration:

rblsmtpd is an RBL SMTP Daemon. It sits between tcpserver and qmail-smtpd and rejects connections from systems identified on one of these lists.

For example, to run rblsmtpd under tcpserver, try something like:

```
#!/bin/sh
QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 2000000 \
  /usr/local/bin/tcpserver -v -R -H -l 0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
    -u "$QMAILDUID" -g "$NOFILESGID" 0 smtp /usr/local/bin/rblsmtpd\
    -r relays.ordb.org /var/qmail/bin/qmail-smtpd 2>&1
```

You can also use multiple RBL database. Popular RBLs are

NAME	Full Name
XBL	Spamhaus Block List
SBL	Spamhaus Exploits Block List
SBL & XBL	Both SBL & XBL together
Spamcop	Spamcop Block List
ORDB	Open Relay Database

APPENDIX-III

SpamAssassin – anti-spam tool

It is an open source tool licensed under the Apache License 2.0. It is a complete set of tools which can prevent spam through various methods like header check, message content, RBL. It is freely available under all Linux distributions. It can be integrated with all major MTAs like sendmail , qmail, postfix. As mentioned above, *SpamAssassin* verifies mail header, message content, DNS blacklist etc. and makes modifications in the header of the configuration. Default, configuration files of spamassassin available at /etc/mail/spamassassin and rules files are in /usr/share/spamassassin. For generating a default local.cf file with default options Michael Moncur has written a very good tool which will generate a local.cf file. Before customizing spam scanning rule, remember NOT to add your rules to any *.cf files in /usr/share/spamassassin. Because when one upgrades *SpamAssassin*, all the existing rules will be replaced by the new default rule sets. So put all your customized rules in /etc/mail/spamassassin/local.cf file. The rules defined in local.cf file are applicable to all users.

Example of local.cf file :

```
# how many hits before a message is considered spam.
required_hits          5.0

# whether to change the subject of suspected spam
rewrite_subject        0

# Text used to  rewrite_subject
subject_tag            ***** LIKELY SPAM *****

# encapsulate spam in an attachment
report_safe            0

# Enable or disable network checks
skip_rbl_checks        0
ok_languages           en

# Mail using locales used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_locales             en
```

Customized rules :

```
body MYRULE_DRUGS /\bviagra\b/I
describe MYRULE_DRUGS Body contains word viagra
score MYRULE_DRUGS 5.5 (if your default threshold is 5)
```

The above rule will match any combination of upper or lower case that spells "viagra" surrounded by work breaks of some form. Similarly you can configure customized header rule like

```
Header MYRULE_DRUGS_SUBJECT =~ /\bviagra\b/I
```

In the above rule, the first part before =~ indicates the name of the header you want to check is and rest is explained above. For more details about regular expression, visit http://www.perldoc.com/perl5.6/pod/perlre.html .

Procmailrc configuration to deliver tagged spam mail to individual user's mailbox like yahoo's bulk mail folder.

Procmailrc serverwide :

```
:0fw
| /usr/bin/spamc
```

Procmailrc for user:

Save the file as .procmailrc in user's home directory.

```
HOME=$HOME
:0:
* ^X-Spam-Status: Yes
$HOME/mail/spammail
```

APPENDIX-IV

POSTFIX WITH SPF

First, download the policy daemon from spf website do the necessary changes. One needs to modify master.cf and main.cf file. This is done for testing purpose. Users are requested to read the document before using it.

Following line added in master.cf file :

IP address of mail server:9998 inet n n n - - spawn user=nobody argv=/usr/libexec/postfix/smtpd-policy.pl

Following modification in main.cf :

smtpd_recipient_restrictions=permit_mynetworks,reject_unknown_client,
check_policy_service inet:IP address of mail server :9998,reject_unverified_recipient

The smtpd-policy.pl script has all the information about the changes required in both the files.

APPENDIX-V

Antivirus Add-ons – Qmail-Scanner and Mail Scanner

- ***MailScanner for postfix :***

  Download the latest distribution and unpack it into the destination directory with a command such

  tar –xvf **`MailScanner*.tar`**

- *Postfix Configuration :*

In the postfix configuration add the following line in /etc/postfix/main.cf:

header_checks = regexp:/etc/postfix/header_checks

In the file /etc/postfix/header_checks add this line:

```
/^Received:/ HOLD
```

For more details, visit http://www.sng.ecs.soton.ac.uk/mailscanner/install/

- ***Qmail-Scanner for qmail :***

  Download the latest distribution and unpack it into the destination directory with a command such as:

  tar –xvf **`qmail-scanner*.tar`**

  ```
  ./configure –-help – To see other available options
  ```

- *Example of qmail Configuration :*

  In the qmail configuration add the following lines in /etc/tcp.smtp:

  ```
  # Use Qmail-Scanner with SpamAssassin on any mail from the
    rest of the world
  ```
  :allow,QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"

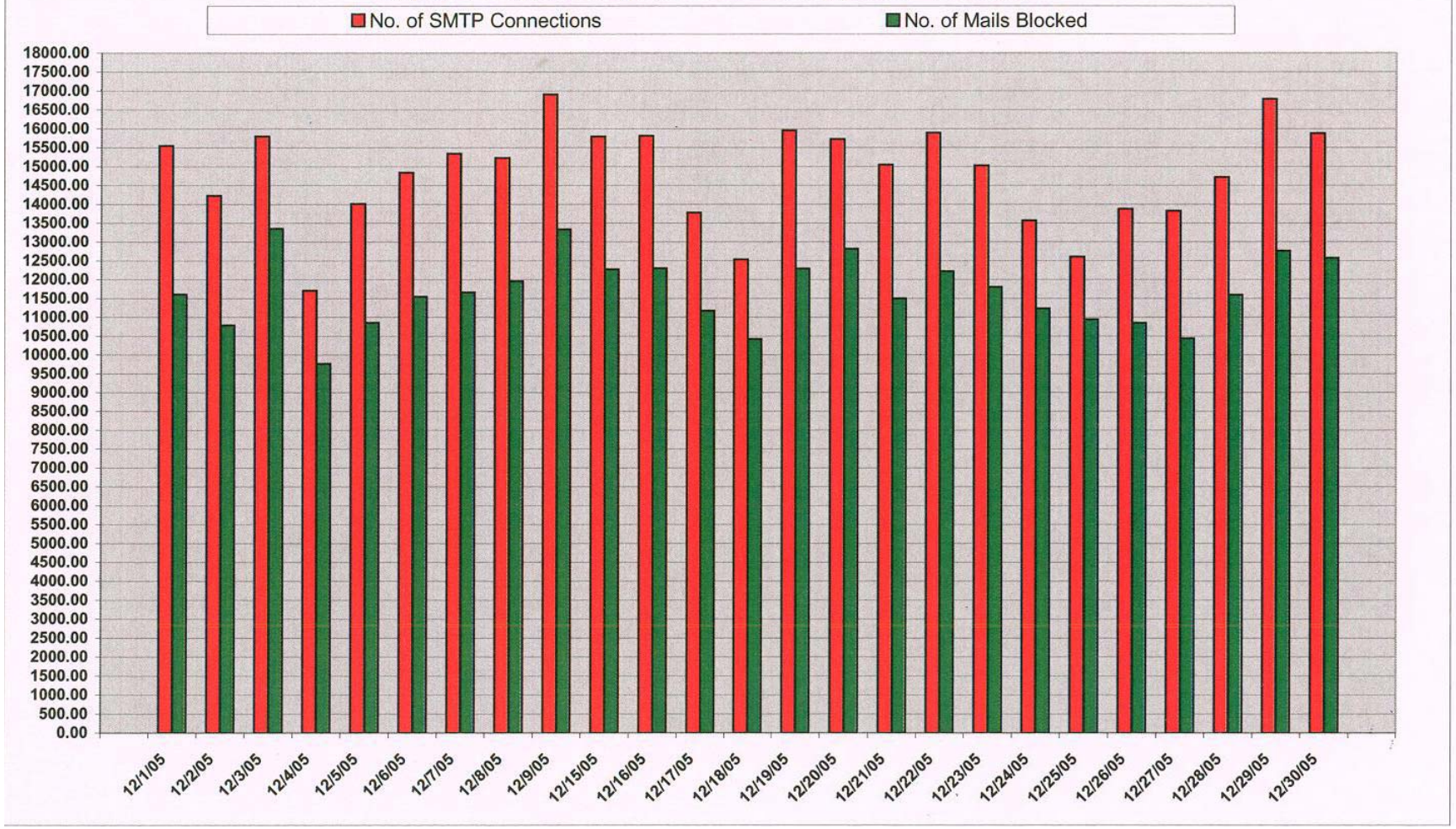
  OR

  :allow,QS_SPAMASSASSIAN="on"

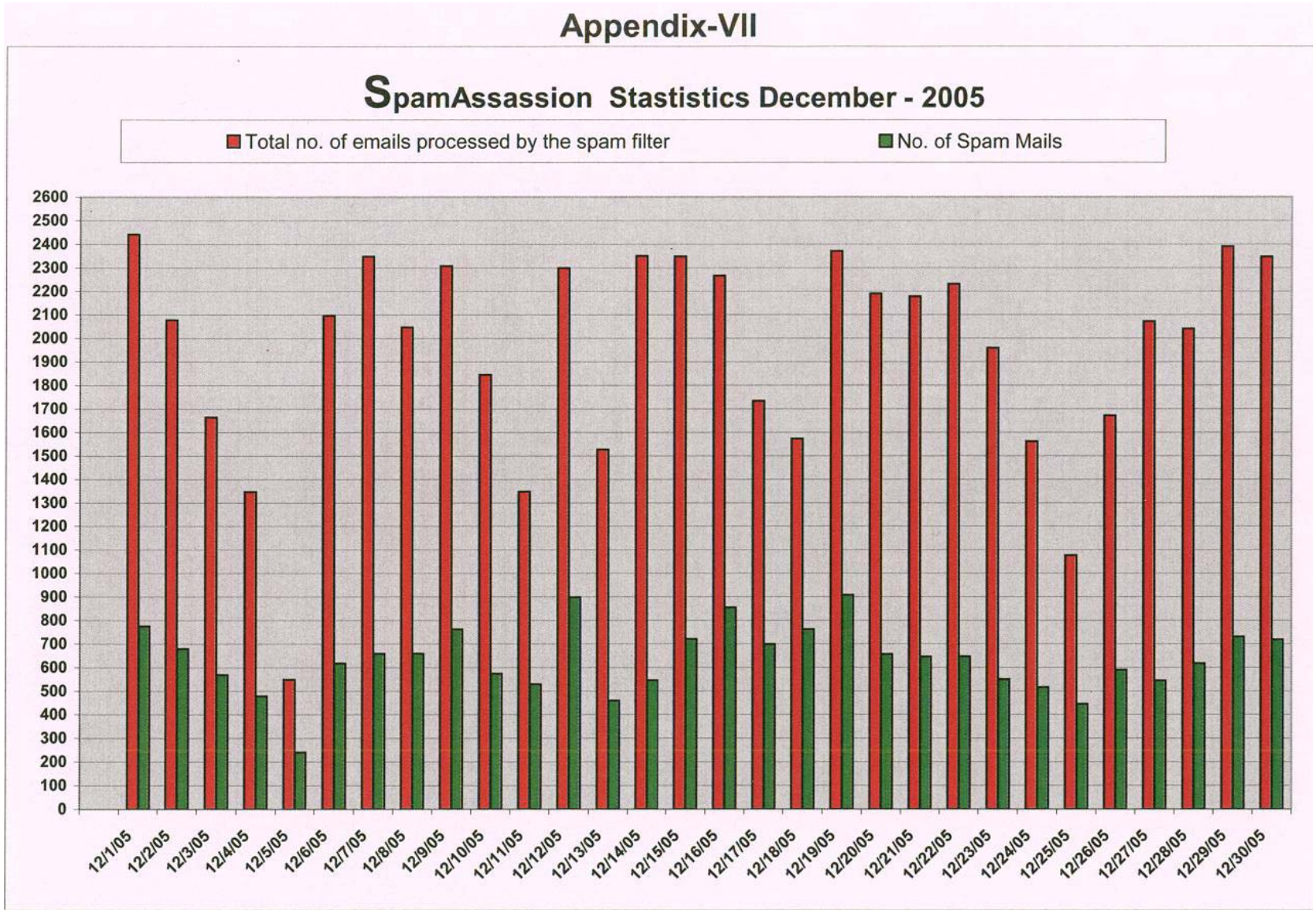
For more details, visit http://qmail-scanner.sourceforge.net/

Appendix-VI

RBL Statistics December 2005



Appendix-VII



3. Conclusions

This report has outlined some methods for implementing antispam and antivirus solutions. Protecting email system with spam, viruses and other malware is imperative for any organization. An effective email security technique must be able to provide the organization with a multi-faceted approach to fighting spam, viruses and malware.

Spam is a problem that is continuing to grow day by day. It is the latest scourge of the Internet, second only to viruses and other malicious codes. There are various techniques available to combat spam. Due to ever-increasing surge in volumes and sophistication of spam, it is critical to choose the most effective spam detection techniques. Every technique has advantages and disadvantages, as well limitations. It is a never ending battle to keep up with the latest spam created specifically to evade content filters. To maximize effective and accurate spam control, antispam solutions will need to combine various layers of protection against both known and unknown spam while minimizing false positives.

Antivirus scanning can effectively become a method of preventing viruses from entering the system. A virus scanning solution is certainly an effective tool to be included as part of any organization’s overall antispam and antivirus management.

4. Acknowledgements

My special thanks to Mr. G.G. Dholakia, Head, PRL Computer Center, for in-depth technical discussions during this work and for his critical comments and suggestions during the preparation of this report. Mr. A.D. Bobra, Prof. Utpal Sarkar and Mr. D.V.Subhedar helped with their comments and suggestions as also my colleagues, Mr. Subhasis Mahapatra, Mr. Hitendra Mishra and, Mr. Alok Srivastava, whose contributions are gratefully acknowledged.

5. REFERENCES

(1) www.qmailrocks.org
(2) www.lifewithqmail.org
(3) www.postfix.org
(4) http://spamassassin.apache.org
(5) PC-Quest, September 2005
(6) http://en.wikipedia.org -- Wikipedia, the free encyclopedia
(7) http://mmmservices.web.cern.ch/mmmservices
(8) www.cert.org
(9) http://qmail-scanner.sourceforge.net/
(10) http://www.sng.ecs.soton.ac.uk/mailscanner/install
(11) http://www.qmailrocks.org
(12) http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

6. Glossary

MTA – Mail Transfer Agent

MDA – Mail Delivery Agent

MUA – Mail User Agent

CERT – Computer Emergency Response Team

SPF – Sender Policy Framework

RBL – Real Time Blackhole List

SURBL – Spam URI Realtime Blackhole List