Solving big problems with Open Source: e-mail

Bill Moran
Potential Technologies
wmoran@potentialtech.com
http://www.potentialtech.com

Creating the perfect mail server

Overall purpose is to minimize unwanted bandwidth usage, as well as minimize productivity loss due to unwanted email.

1) Will refuse to deliver unwanted mail while reliably delivering legitimate mail.
2) Extremely low incidence of false tagging regarding #1.
3) When false tagging occurs, it must be obvious so corrective action can be taken.
4) This must not create additional work for the user.
5) No mail may ever be lost.
6) Must not generate collateral spam.
7) The entire system should use Open Source components.
8) We are operating under the understanding that email is not always the proper method for communication.

What is unwanted mail

- Virus/worms: malicious programs of any type.
- UCE (spam): Bulk mailings of any type, that are **not** requested by the recipient.
- Collateral spam (backscatter mail): reject/bounce notices caused by other protection systems when our domain is forged as the source address.

False Positives

A false positive is when an email is incorrectly flagged as an unwanted email.

Why are they bad

- Inconvenience to sender, recipient or both
- Often times message gets lost (more ...)

Messages should never get lost!

- Systems for filtering unwanted email should **NEVER** delete an email.
- Often, filtering systems will put suspect email in a special location, to be reviewed by the intended recipient. This is inconvenient, and likely to cause mistakes.
- Many systems strip certain attachments (as a virus protection measure). This is almost as bad as deleting.

False Negatives

- Inconvenience user
- Potential of damage if false negative is a virus or worm

Acceptable amount of false tagging

- False positives are the worst, as they delay communication and make interacting with clients difficult. They could even cause us to lose business.
- False negatives are usually annoying at worst, but could be dangerous when virus/worms are involved. However, a secondary protocol is established to protect against those (virus protection at workstation level)

False tagging should be obvious and easy to correct

- False negatives on UCE are usually pretty obvious and require the user to delete the message. Reports may also be filed via Spamcop.
- False negatives on virus/worms are caught by virus protection on Windows workstations, or treated the same as spam on POSIX systems.
- False negatives on collateral spam are a problem area.
- False positives must result in noticeable bounce messages to the messages originator. There must be an easy way for victims of false positives to report the incident, and for the postmaster to correct the problem.

Mail must never be lost

- Mail can never go to /dev/null
- The user should not be burdened with searching multiple folders to see which contain legit mails and which don't.

We must not generate collateral spam

- How: Mail will never be accepted if it will not be delivered!

Results:

- With no measures taken:
  2.54 spams/hour, 0.85 worms/hour
- With all measure in place:
  0.02 spams/hour, 0 worms/hour
- The current configuration has not generated any false positives in several months.

Software Used:

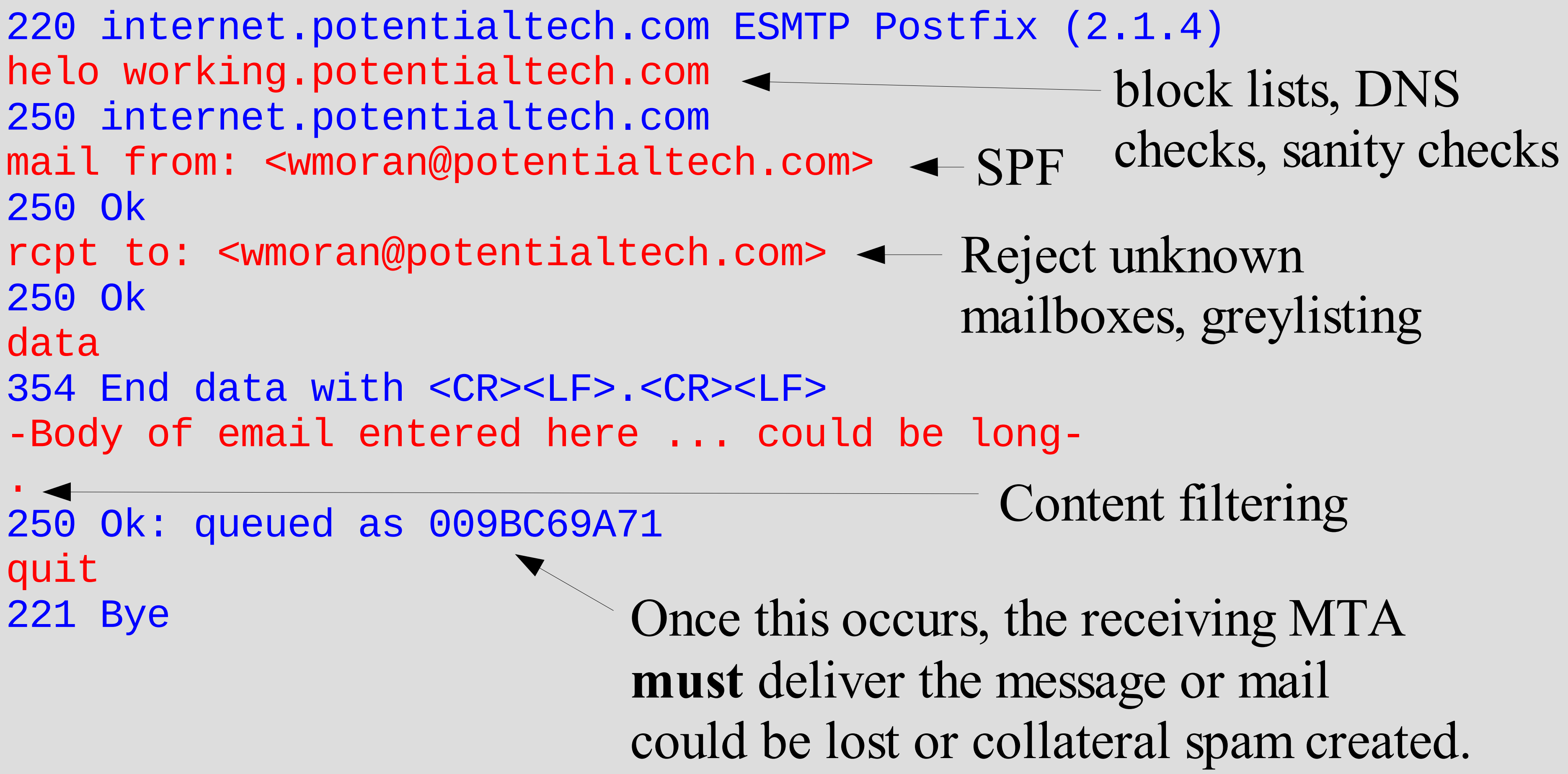
- FreeBSD 4 http://www.freebsd.org
- Postfix 2.1 http://www.postfix.org

Software Considerd for Improvements:

- Posgrey http://isg.ee.ethz.ch/tools/postgrey/
- ClamAV http://www.clamav.net
- Spamassassin http://spamassassin.apache.org/

Where do we detect?

- To avoid lost mail and collateral spam, all checks must be done prior to completion of the SMTP dialog:



```
220 internet.potentialtech.com ESMTP Postfix (2.1.4)
helo working.potentialtech.com
250 internet.potentialtech.com
mail from: <wmoran@potentialtech.com>
250 Ok
rcpt to: <wmoran@potentialtech.com>
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
-Body of email entered here ... could be long-
.
250 Ok: queued as 009BC69A71
quit
221 Bye
```

block lists, DNS checks, sanity checks

SPF

Reject unknown mailboxes, greylisting

Content filtering

Once this occurs, the receiving MTA **must** deliver the message or mail could be lost or collateral spam created.

Checking the sanity of the sending server:

- Ensuring that RCPT TO: adheres strictly to RFC-821 format
  `strict_rfc821_envelopes`
- Reject unauthorized use of pipelining (sending the next command prior to a response from the previous)
  `reject_unauth_pipelining`
- Reject completely bogus hostnames
  `reject_invalid_hostname, reject_non_fqdn_hostname`

Effectiveness of Sanity checks

- With no filtering:
  2.54 spams/hour, 0.85 worms/hour
  3.29 unwanted emails/hour
- With Sanity checks only:
  0.77 spams/hour, .17 worms/hour
  0.94 unwanted emails/hour

Block Lists

- Block lists allow you to use community-maintained lists of known junk mail sources to reject email:
```
reject_rbl bl.spamcop.net
```
- spamcop.net, ordb.org, spamhaus.org, relays.orirusoft.com, njabl.org
- Spamcop has the added advantage of allowing the average user to do something effective about the problem.
- 1.14 spam/hour, 0.29 virus/hour
  1.33 junk mails/hour

Local Server Blocklists

- Based on policy, we are able to establish hosts that have a low likelihood of ever sending us useful communications, but can be seen to be persistent junk mail problems:
  `check_client_access hash:/path/to/list1`
- These lists are manually maintained on an as-needed basis (basically, a reaction to what gets past other filters)
- At time of testing: 96 domains listed
- 2.10 spam/hour (17%)
  0.40 virus/hour (52%)
  2.50 total junk mail/hour (26%)

SPF
(Sender Policy Framework)

- Uses special DNS entries to list servers that are valid origins for mail.
- Gives you a way to publish information that other mail systems can use to identify forgeries and reject them.
- Allows you to check incoming mail for forgeries.
- Both the receiver and the domain listed in the MAIL FROM: command must support SPF for it to be used.
- http://spf.pobox.com

How SPF works

- Special DNS records for each domain list the servers that are authorized to send mail for that domain.
- Once you have the hostname for a server, and the email address from which the mail is (supposedly) being sent, you can validate these against the SPF records.
- If the information doesn't validate, then the mail is being sent via an unauthorized server, and is likely forged.
- In this way, it reduces junk mail as well as protecting you domain from forgeries and collateral spam.

Our implementation

- potentialtech.com publishes SPF records.
- mail.potentialtech.com does not check SPF records
- mail.potentailtech.com uses SMTP AUTH over TLS, so there is no reason to send mail through any other server.

Effectiveness

- We receive so little collateral spam that it would be difficult to establish statistics.
- Effectiveness of SPF will depend on it's level of adoption by ISPs.

The correct way to reject mail for nonexistent mailboxes

```
220 internet.potentialtech.com ESMTP Postfix (2.1.4)
helo working.potentialtech.com
250 internet.potentialtech.com
mail from: <wmoran@potentialtech.com>
250 Ok
rcpt to: <fred@potentialtech.com>
550 <fred@potentialtech.com>: Recipient address rejected: User unknown
```

- This does not generate collateral spam.
- This avoids putting the load of generating a bounce message on the mail server.
- Keeps the queue clean of undeliverable messages.

Why 3rd party SMTP relays are bad

- They do not know your user list, and will thus accept mail that you will need to bounce, often creating collateral spam.
- They do not use the same junk mail protections, and thus create a hole through your checks.
- They don't provide any truly tangible benefit in many cases.
- That being said, there **are** situations where backup SMTP is beneficial, and it **is** possible to configure it correctly.

greylisting: what it is

```
220 internet.potentialtech.com ESMTP Postfix (2.1.4)
helo working.potentialtech.com
250 internet.potentialtech.com
mail from: <joe@potentialtech.com>
250 Ok
rcpt to: <wmoran@potentialtech.com>
450 <wmoran@potentialtech.com>: Recipient address
 rejected: Please try again soon.
```

- 450 is a temporary failure, the same failure message that would be returned if the server were simply too busy to handle the mail at this time, or the mailbox were full.
- Any correctly designed mail server will wait a short while, then retry the message.
- The greylist program will store the details of this message in a database, and on the next attempt that the same server tries to send using the same `from` and `to` addresses, it will be allowed (usually only after a certain time period has elapsed)

Why greylisting works

- Viruses with embedded SMTP systems are too simple to remember to resend and treat 450 the same as 550 (postfix queue manager is 6000 LOC).
- Many bulk-mailing programs (such as spam zombies) also treat 450 the same as 550: resending would defeat the purpose of mass mailing or over-complicate the software.
- Many spam/virus origins generate a random FROM address on each attempt, thus they are greylisted forever.
- When used in combination with block lists, the grey list delays mail until the block lists learn about the new junk mailer and list it.

Concerns regarding greylists

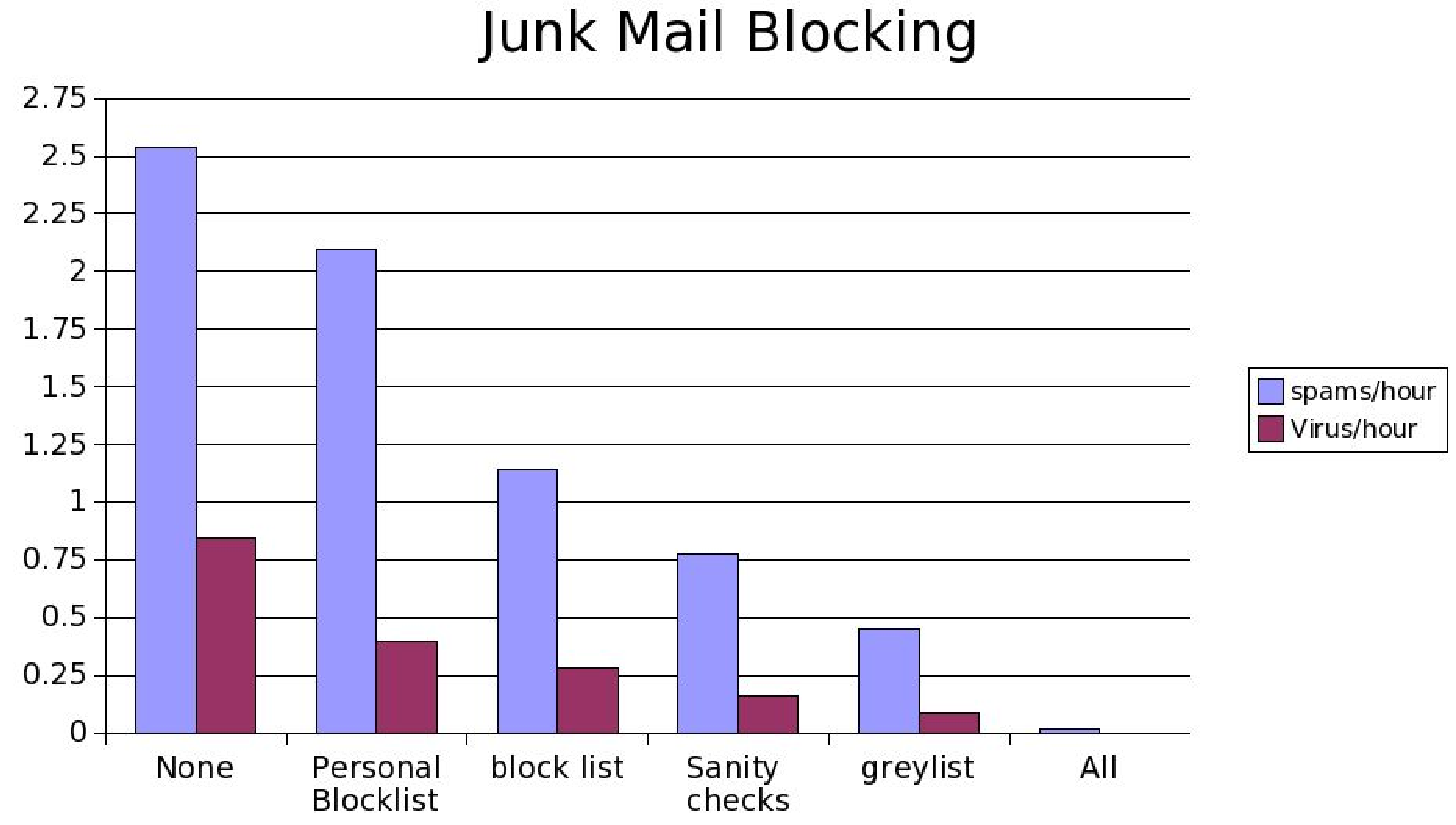
- Mail will be delayed unreasonably long:
  In actual practice, we've seldom seen greylisted mail take longer than 15 minutes to be resent. Frequent senders are always in the db, and never delayed.
- The database lookup will be slow:
  Lookups are less than 1s on an 800mhz
- Database size will soak up all my HDD:
  Database size: 100M -> ISP w/ ~675 users
  Database reaches an equilibrium as old records are garbage collected
- Legit, broken servers will be unable to send!:
  White lists for broken servers are publicly available, list is currently shorter than 20 domains

Effectiveness of greylisting

- With no measures taken:
  2.54 spams/hour
  0.85 virus/hour
  3.39 total junk mails/hour
- With greylisting only:
  0.63 spams/hour (75%)
  0.13 virus/hour (85%)
  0.76 total junk mails/hour (78%)

Some greylist software

- Postfix ships with a simple greylist program.
- Postgrey is a full-featured greylist program specifically for Postfix.
- RelayDelay works with sendmail.
(See http://www.freebsd.org/docs/ for a well-done article by Tom Rhodes)


Junk Mail Blocking
2.75
2.5
2.25
2
1.75
1.5
1.25
1
0.75
0.5
0.25
0
None
Personal Blocklist
block list
Sanity checks
greylist
All
spams/hour
Virus/hour

Discussion of filters not used

- Aggressive DNS validation
- SPF checks
- Content filtering
- “Send me a verification” systems

Failure of aggressive DNS validation

- hostname announced on HELO must resolve via DNS.
  `reject_unknown_hostname`
- IP address must reverse resolve to something, and that something must forward resolve.
  `reject_unknown_client`
- No actual numbers, but this was very effective a blocking spam and viruses.
- Unfortunately, it was also very good at generating false positives.

SPF checks not implemented

- Effectiveness of other techniques make the complexity of SPF checks unnecessary.
- I know of no mail server that natively implements SPF checks, so additional software would have to be installed, configured, and maintained.

Content filtering

- Virus filters:
  Compare attachments (and things that look like attachments) to profiles of malicious software.
- spam filters
  Take a number of forms, but usually compare a large number of criteria to the message, and use a scoring system to establish the likelihood that the mail is spam.

General Problems with Content Filtering

- Content filters generally require a large amount of RAM and a large number of CPU cycles. This requires a more powerful server to accomplish.
- Generally the server must be intentionally throttled to prevent incoming mail from overloading the system In times of peak load, the throttling can cause unusual mail delays.
- Lack of throttling can cause the MTA to be overloaded.
- In order to prevent collateral spam and undeliverable bounce messages, the SMTP session must wait for the filter to complete.

More general problems with Content filters

- Content filters are high-maintenance in that they require constant updating to keep up with the latest spam/worm profiles.
- Spammers are constantly changing their MO in a direct attempt to defeat content filters.

Advantages of content filters over other techniques

- Other systems discussed here do not catch junk mail that is forwarded by another server or a mailing list.
- Some viruses and spammers hijack legitimate mail servers to spread, these can often get past the other techniques.

Popular Content Filters

- ClamAV: Virus filter
- Spamassassin: popular rule/score-based spam analysis

Send me a nother email to prove you're not a bot

- Works by keeping a database (similar to a greylist) of known-good senders, and requiring an unknown sender to verify themselves (much the way most MLMs handle subscriptions)
- Creates extra work for the sender.
- Requires extra software installed/maintained on the server.
- Generates collateral spam.

Whitelists: the key to confidence in filtering

- Whitelists allow you to filter, yet still feel confident that important email will never be blocked
- User whitelists allow you to block entire ISPs while still letting important users get through
- server whitelists allow you to ensure that important servers (such as client's mail servers) are never blocked or delayed.
- Some legit mail servers react badly to greylists, thus you should have a whitelist that bypasses greylisting.

The End

This presentation will be available:
http://www.potentialtech.com/wmoran/