Specially Prepared Advertising Material
How do we manage it?

Andy Linton

asjl@citylink.co.nz

CityLink Case Study

- What's the problem with SPAM?
- Who are we?
- What systems do we run?
- How well does it work?

What's the problem with SPAM

- There's lots of it
- We almost certainly don't want most of it
- It can be hard to identify
- If you can identify it well you can
  - Mark it for users to deal with
  - Throw it away
  - Don't send it back!

Who are we?

- An open access fibre and ethernet provider
- We're NOT an ISP or a telco
  - We don't provide mail for customers
- Small company with about 30 staff
  - Mail is critical to our business
  - Need to be able access mail in the office and at home

What systems do we run?

- Operating Systems
  - Servers
    - Windows Server 2003
    - Linux - Debian and Ubuntu
  - Desktops
    - Windows XP
    - Linux - Debian and Ubuntu
    - Mac OS X

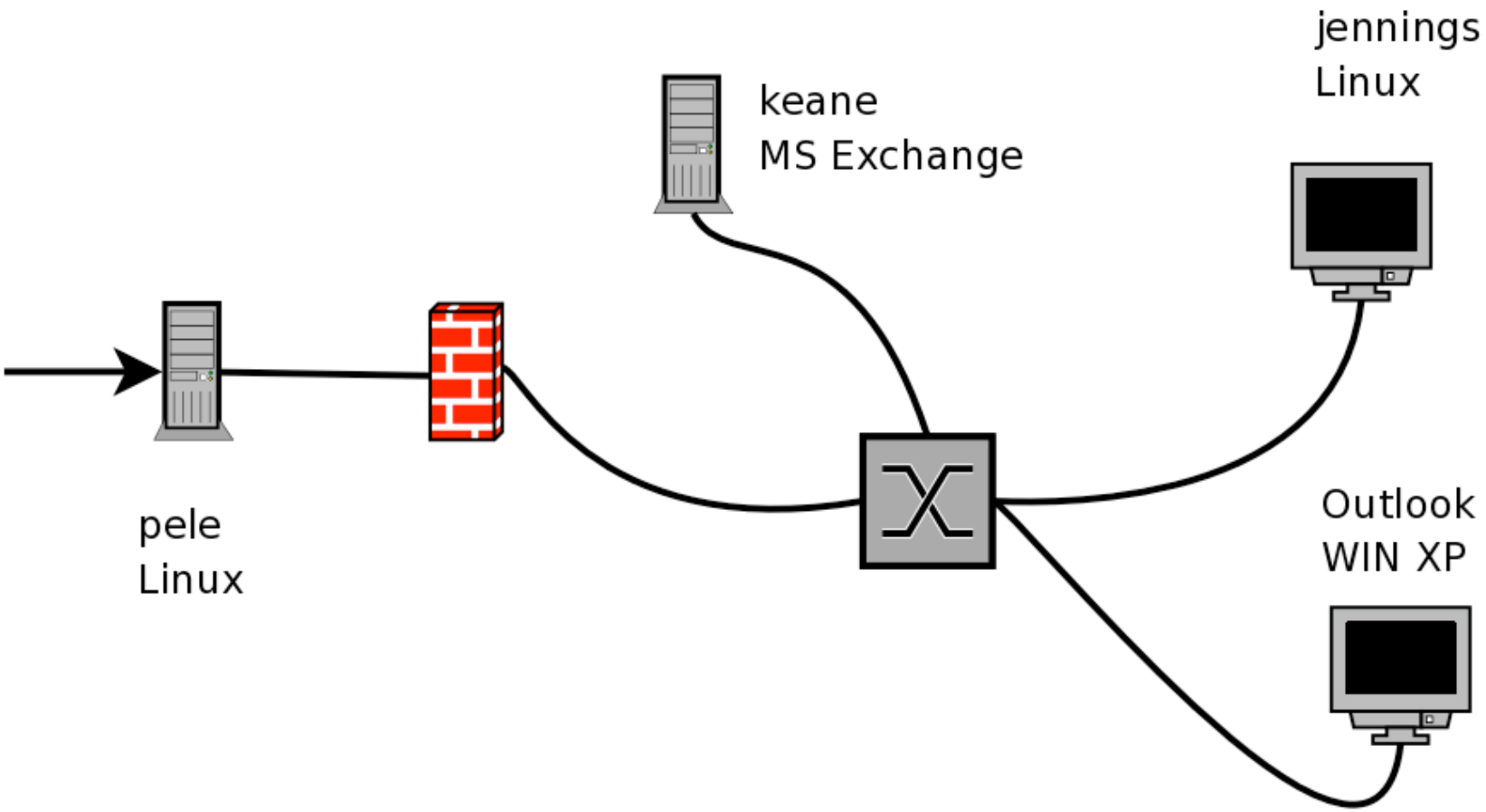
What mail server software do we run?

- Microsoft Exchange
- Postfix
- Exim4

What mail applications do we run?

- Microsoft Outlook
- Thunderbird
- Evolution
- Mutt
- Pine
- Squirrelmail
- And……?

How does it fit together?



Linux server - pele

- Postfix
  - Postgrey
  - Reject mail for users that don't exist
  - Amavis http://www.amavis.org/
    - Clamav http://www.clamav.net/
    - Spamassassin http://spamassassin.apache.org/
      - FuzzyOCR http://fuzzyocr.own-hero.net/
  - .mailfilter to run Spamassassin again on per user basis
  - Maildrop to deliver to local disk or Exchange server

Postfix

- Available as a package for range of *nix systems
- Very flexible configuration
- http://www.postfix.org/

Greylisting mail

- Software looks at:
  - The IP address of the host attempting the delivery
  - The envelope sender address
  - The envelope recipient address
- If we have never seen this triplet before, then refuse this delivery and any others that may come within a certain period of time with a temporary failure.
- http://projects.puremagic.com/greylisting/links.html

Reject mail for users that don’t exist

```
# The unknown_local_recipient_reject_code
# specifies the SMTP server response code The
# default setting is 550 (reject mail) but it is safer to
# start with 450 (try again later) until you are certain
# that your local_recipient_maps settings are OK.

#unknown_local_recipient_reject_code = 450
unknown_local_recipient_reject_code = 550
```

Amavis

- Scans mail for viruses and spam using spamassassin
- Software set up to retrieve updated Clamav virus definitions on a regular basis
- Once it’s set up it’s low maintenance

Spamassassin

- Applies a series of tests on each message
  - If score exceeds a threshold then it gets marked as SPAM
- We use SARE (Spamassassin Rules Emporium) to download new rules daily
- http://www.rulesemporium.com/
- We also use OCR to look at images

Putting it all together

- How To Install Postfix, Amavis, ClamAV, and Spamassassin
- http://www.fatofthelan.com/articles/articles.php?pid=22

How well does it work?

- We think it works well but….
- It wouldn’t scale for a large ISP without tuning
  - In use today at IUSN, Niue
- Good illustration of Unix tools approach
- Principles apply if you use other mail software
- “When in doubt, use brute force”
  - Ken Thompson, Bell Labs

Sender Policy Framework

- Today, nearly all abusive e-mail messages carry fake sender addresses. The victims whose addresses are being abused often suffer from the consequences, because their reputation gets diminished and they have to disclaim liability for the abuse, or waste their time sorting out misdirected bounce messages.
- http://www.openspf.org/Introduction

Setting up an SPF record

- See the set up wizard on this page
  - http://www.openspf.org/Project_Overview

Conclusions

- There’s no magic solution that solves the problem
- The spammers are constantly changing their tactics - you need to do the same!!
- The first 90 percent accounts for the first 90 percent of the effort. The remaining 10 percent accounts for the other 90 percent.

Questions?