

# Spam from an ISP perspective

Simon Lyall, Ihug

Uniforum NZ NetForum Conference  
July 2003

# Who is Ihug?

- 3<sup>rd</sup> largest ISP in New Zealand
- 90,000 dialup and broadband customers
- Email System software: Exim, qmail, openldap on Debian Linux.
- Email system spread across 14 servers.
- Duplicate system in Australia.

# The Scale of the Problem

Total emails received each day 1,250,000

Estimate Legitimate Emails per day 400,000

Estimated Spam Emails per day 560,000

Sent to invalid addresses 270,000

Proportion of email that is Spam 60%

# Spams Blocked per customer

Percentile	Spams/day	Unblocked
50	15	2
60	20	2
80	35	4
90	60	7
95	85	9
99	150	17

# Mid 2004 on Current trends

- Total Email volume has doubled in 12 months
- 90% of each customer's email is Spam
- Anti-Spam solutions need to block 95-98% of Spam
- 2004's Spam has evolved to beat 2003's filters

# If 10% monthly growth for 12 months

Percentile	Spams / day	Unblocked
20	18	2
50	46	5
80	108	12
90	186	21
95	264	29
99	465	52

# History of Spam Filtering at Ihug

Before 2000	Little or no filtering
2000 - Feb 2002	MAPS RBL+
2002 - Jun 2003	MAPS RBL+ & Spamcop
Jun 2003 - present	Spamassassin based

# Why ISPs care about Spam?

- Customers Unhappy
  - Close accounts
  - Blame the provider
  - Call helpdesk
  - Install their own anti-spam software
- Resources Wasted
- Staff unhappy/offended/wasting time
- Money to be made

# Customer expectations of Mail and Anti-Spam system

- *All email must go through instantly*
  - Bouncing or deleting suspected spam is not an option
  - False positives must be kept to an absolute minimum
- *Except the mail I don't want*
  - 100% hit rate is expected
  - Each customer's definition of Spam is unique
- *Must be free and involve no work for me*
- Must be optional

# Technology for Blocking Spam

- External Solution Providers
- DNSBLs
- Other methods

# External Providers

- Pros

- Brandname Product
- Support
- Pretty Effective

- Cons

- Cost
- Not 100% effective
- Implementation costs

# DNS Block Lists (DNSBLs)

- Used to check IP of sending server
- VERY wide variety of DNSBLs and organisations running them.
- Wide range in quality, goals and usefulness.
- Spam Blocking vs Behaviour Changing vs Group of Networks

# Types of DNSBLs

- Open Relay (ORDB)
- Open Proxy, Open formail (monkeys.com)
- Country or Provider based (blackholes.us, Cluecentral)
- Dialup and Dynamically assigned Ips (MAPS DUL)
- Known Spammers, Spam friendly ISPs, slow reacting ISPs (Spews, Spamhaus SBL)

# Types of DNSBLs (cont)

- Current Spam (bl.spamcop.net , MAPS RSS)
- Whitelists (bondedsender.org)
- Other
  - Random
  - Everything
  - Very aggressive
  - Specific
  - Private

# Using DNSBLs

- Read the listing and delisting criteria
- Don't use duplicate lists
- They ALL make mistakes
- Some make more mistakes than others
- Make sure the list's values align with yours
- Mirror the lists locally to cut down on delays

# Other Technologies

- Distributed Checksums (Razor, DCC)
- Suspicious Connection Throttling
- Marking non-Spam
  - Habeas
  - Bonded Sender
  - Challenge response (Earthlink, Actrix)
  - Force lists to register (AOL)

# Other Technologies (cont)

- Bayesian
  - Paul Graham article
- Rules Based
  - Procmail
  - Spamassassin
  - Spambouncer

# Integrating Spam filtering

- It must be optional.
- Customers must be able to examine and retrieve deleted email
- Remember each customer is different
- Plan beforehand what to do about mistakes
- Aim to block at least 90% of Spam
- Remember to review and upgrade regularly

# Controlling Customers

- Clear AUP
- Ability to suspend and close customers
- Monitored abuse address
- Open relay scanning
- Open proxy scanning
- Port 25 blocking
- Management support

# Questions

- This talk online
  - <http://www.darkmere.gen.nz>

# Links

- External Providers

- Brightmail <http://www.brightmail.com>
- Postini <http://www.postini.com>
- Message Labs <http://www.messagelabs.com>

- RBLs

- Multi RBL lookup <http://www.moensted.dk/spam>
- MAPS <http://www.mail-abuse.org>
- Spamcop <http://spamcop.net/bl.shtml>
- Spamhaus <http://www.spamhaus.org>

# More Links

- Software
  - Spamassassin <http://www.spamassassin.org>
  - Procmail <http://www.procmail.org>
- Bayesian Filters
  - Paul Graham <http://www.paulgraham.com/spam.html>
  - Bogofilter <http://bogofilter.sourceforge.net>
- Reporting Spam
  - Abuse.net <http://www.abuse.net>