

Fighting SPAM@MLC


Mark Szidik, CIO
Michigan Library Consortium



In the Beginning was the key

- Delete key was our only defense
- Annoyance level was fairly low for all staff
- Low administrative overhead

Users get frustrated

- Early 2002 many user complaints
- Users doing dumb stuff (reading SPAM)
- Volume of SPAM rising
- Sophistication of SPAM rising
-  key no longer strong enough defense

May 2002 SpamCop installed

- User complaints cross my annoyance threshold
- I needed a quick-fix to the SPAM problem
- SpamCop was simple to install and cheap (free) to acquire
- Worked well (for a while)

SpamCop

Good News:

- Some SPAM was being blocked
- users quieter

Bad News:

- False Positives
- Reliability problems

SpamCop – the end

- SPAM volume still rising
- Users still doing dumb stuff
- Major outage of SpamCop in August of 2003

Enter SpamAssassin

- Started testing in October 2003 on 2 users
- More work to configure
- Many more features
- Very effective
- Full production in December 2003

SpamAssassin vs. SpamCop

- SpamCop is a blacklist and only looks at sender domains/IP's
- Blocks SPAM at mail host
- SpamAssassin filters based on mail content
- Flags SPAM, does not block SPAM

SpamAssassin Setup

- A lot more work
 - Setup Procmail recipe for each user
 - Setup of .forward file for each user
 - Frequent tweaking of config
- A lot of overhead
 - Running spamd process
 - Spawning spamc process for each incoming message

Virus Scanning

- Clam AntiVirus + ClamAssassin
- Open Source
- Another daemon process (clamd)
- New lines in each users Procmail recipe
- Viruses flagged on subject line

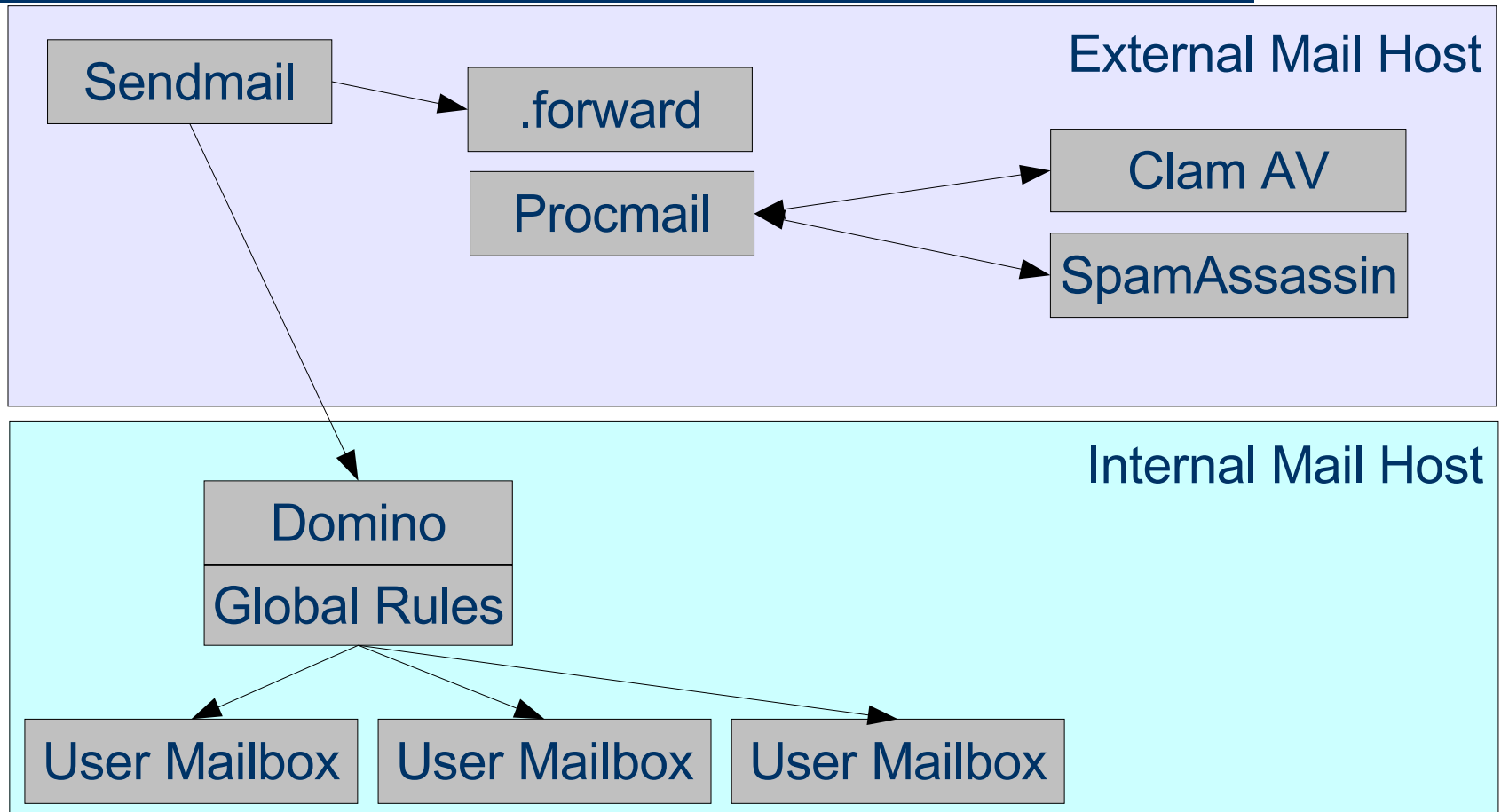
Final Frontier: Mailing lists

- Using Mailman list management system
- Custom handlers (plugins) for Mailman
- Small changes to Mailman config file to pass mail through SpamAssassin, Clam Antivirus
- Viruses are discarded automatically
- SPAM is held for moderator approval

Notes/Domino Antispam efforts

- V5 of Notes/Domino had no features to fight spam
- V6 added global rules (keyword scanning)
- V6.x
 - added blacklist service support in Domino
 - Notes added default junk mail folder, easier rule creation for flagging spam, sender blocking

Message Flow



MLC vs. SPAM: The Score

- Currently identifying 1,100 SPAM's per day
- Identifying 90 Viruses daily
- Ratio of SPAM to legitimate mail: **2.33 : 1**
- False Positives: nearly zero *
- Missed SPAM: 2 – 5 per day per user *

* As reported by users in recent survey