ClamAV
An Introduction

PacNOG I Workshop

June 21, 2005
Nadi, Fiji

Hervey Allen

What is it?

From `http://www.clamav.net/abstract.html`

Clam AntiVirus is a GPL anti-virus toolkit for UNIX. The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multi-threaded daemon, a command line scanner, and a tool for automatic updating via Internet. The programs are based on a shared library distributed with the Clam AntiVirus package, which you can use with your own software. Most importantly, the virus database is kept up to date .

ClamAV – Key Features

Based on: http://www.clamav.net/abstract.html

- *Command-line scanner*
- *Multi-threaded daemon*
- *milter interface for sendmail*
- *Database updater with support for digital signatures*
- *Virus scanner C library*
- *On-access scanning (Linux and FreeBSD)*
- *Detection of over 35000 viruses, worms and trojans*
- *Built-in support for RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (Compressed HTML)*
- *Built-in support for mbox, Maildir and raw mail files*

ClamAV quick facts

- Virus database is updated (average) multiple times per week.
- End-users can submit samples directly: `http://www.clamav.net/sendvirus.html`
- Will detect phishing as malware if you wish.
- *freshclam* daemon runs to keep virus definition up-to-date.
- ClamAV mailing list available: `http://lists.clamav.net/cgi-bin/mailman/listinfo/clamav-users`

Supported platforms

OSes

- Linux
- Solaris
- FreeBSD
- OpenBSD
- NetBSD
- AIX
- Mac OS X
- Cygwin B20

Hardware

- Intel
- Alpha
- Sparc
- Cobalt MIPS boxes
- PowerPC
- RISC 6000

Where does it fit with Exim?

Check for viruses after you've done:

- Blacklists
- Whitelists
- Content-based solution (like SpamAssassin)

Final action is up to you, but generally you'll *deny* any mail that's detected as having a virus.

You'll do this in the *acl_check_data* ACL in the Exim *configure* file.

More resources

- ClamAV online specimen scanner:
  - http://test-clamav.power-netz.de/
- ClamAV main site:
  - http://www.clamav.net/
- The ClamAV FAQ:
  - http://www.clamav.net/faq.html
- The AmaViS (*A Mail Virus Scanner*) Project. An alternative to ClamAV:
  - http://www.amavis.org/