

# FNAL

## Central E-Mail Systems

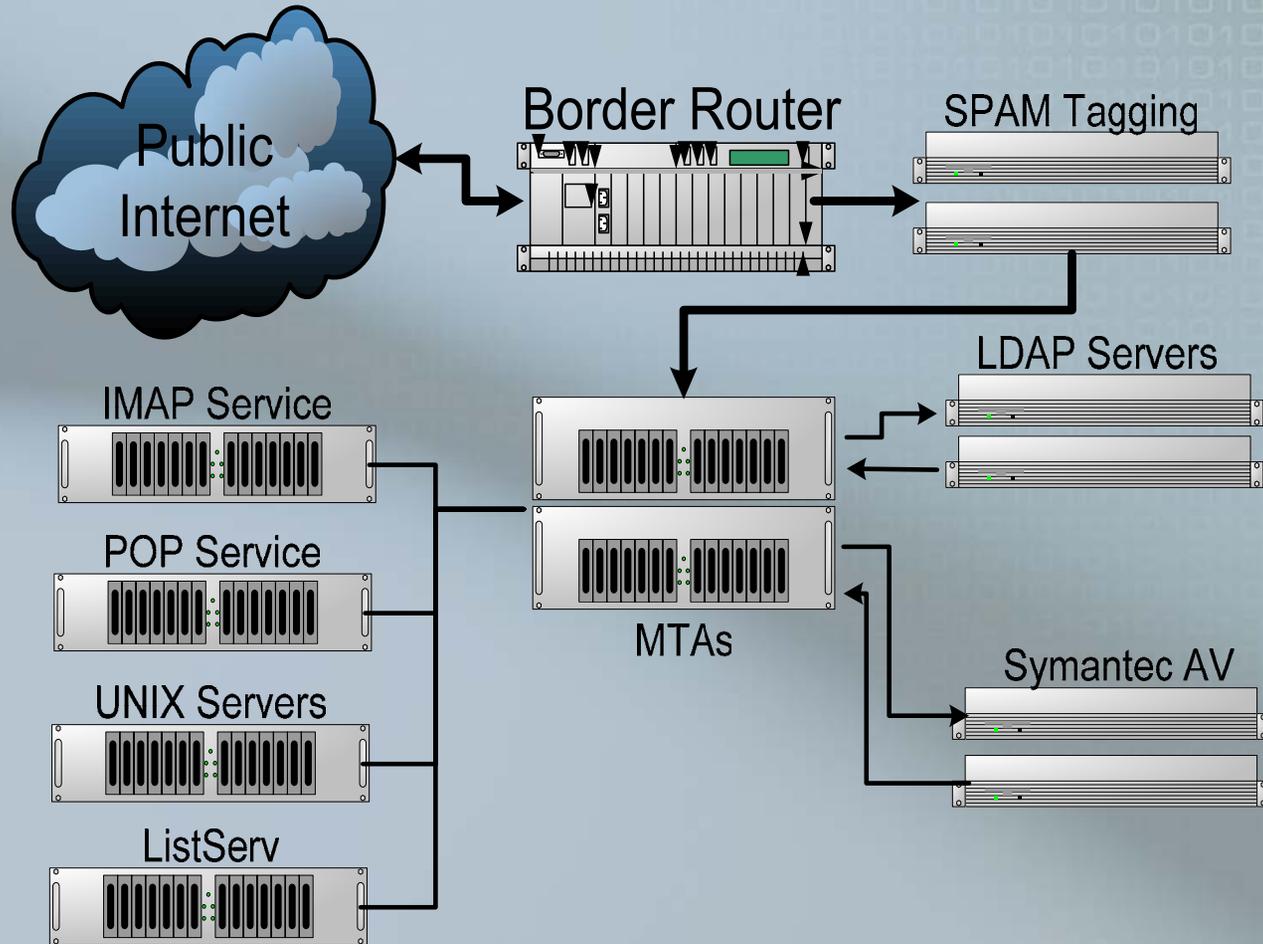
Jack Schmidt, Al Lilianstrom,  
Ray Pasetes, and Kevin Hill

Fermi National Accelerator Laboratory

# Hardware

- SPAM Tagging  
Dell 2650
- MTA  
Sun E280
- LDAP  
Sun Netra
- Symantec AV  
Dell 2650
- IMAP  
Sun E280
- POP  
LSI FC SAN  
Sun Netra  
LSI FC SAN
- ListServ  
Dell 2650

# FNAL E-Mail System Configuration



# Services Software

- Centrally supported services use commercial software. The 'UNIX Servers' represent the various UNIX and Linux machines that choose to receive mail
- IMAP
  - Solaris 9
  - Sun JES Mail Server
- POP
  - Solaris 8
  - iPlanet Messaging Server
- ListServ
  - Windows Server 2003
  - LSoft ListServ

# Gateway Software

- A combination of commercial and open source software is used to build the gateway system
  - SPAM Tagging
    - Fermi Linux LTS 3.01
    - PostFix
    - Spam Assassin
  - MTA
    - Solaris 9
    - SunONE Messaging
    - Sophos AntiVirus
  - LDAP
    - Solaris 9
    - SunONE Directory
  - AntiVirus
    - Windows 2000
    - Symantec NAV

# Incoming Mail

- Mail that is destined for a user at Fermilab can only enter the site through a small number of dedicated machines. All other attempts are rejected
- By imposing this restriction all incoming mail can be evaluated by software designed to check the mail for SPAM indicators and for viral content
- Mail that originates outside of Fermilab for Fermilab users should be addressed to `user@fnal.gov`. If the mail is addressed to `user@machine.fnal.gov` MX records are used to discover that the MTA is the route the mail has to take to get delivered

# SPAM Tagging

- All incoming mail is routed through the SPAM tagging subsystem.
- Based on a combination of PostFix and SpamAssassin the mail is evaluated as potential SPAM as follows:
  - Internal SpamAssassin rules
  - DNS queries sent to public access RBLs (Real Time Blackhole Lists)
  - SpamAssassin 'autolearn'

# SPAM Tagging

- Mail that passes through SpamAssassin is scored
  - X-Headers added with a numeric rating
  - Messages with a score greater than 5 have a X-SPAM-Flag header added with its value set to Yes. This flag can then be used by any client that supports filtering of messages based on headers
- While not 100% effective user response has been very positive.

# MTA

- Once the mail has been processed by the SPAM tagging system it is handed off to the MTA.
  - LDAP lookup to determine the delivery destination
  - Sophos AntiVirus check
  - NAV Check
  - Delivery
- Sophos stops approximately 95 to 98 percent of the viruses that get to Fermilab via email.
  - Any message that is determined to have viral content is not delivered. Neither the sender or the intended recipient is notified.
  - The Sophos definitions are updated two ways: By cron every other hour and via a email from Sophos that a new definition is available.

# MTA

- The MTA is also used as the SMTP server for the desktop clients and as an authenticated SMTP (TLS and SMTP over SSL) server for users who travel to allow relaying of mail
- The MTA processes an average of 800,000 to 1,200,000 messages per week.

# Symantec AV

- Sophos is approximately 95 to 98 percent effective in removing viral content.
- Previous IMAP implementation used Symantec AntiVirus for Gateways on the server to catch any viruses that made it past Sophos
- IMAP service design change allowed us to implement Symantec AV as a service for all mail that comes through the gateways
- This has resulted in nearly all viruses being caught before they reach the users mailbox. The Symantec definitions are updated every other hour

# IMAP Services

- Preferred method for users at Fermilab to receive mail
- Centrally managed and supported service
- Users are not restricted to a particular client and a webmail interface
- User information stored in redundant LDAP servers

# IMAP Services

- Mail resides on SAN available via redundant paths
- Higher quotas available for mail retention
- Server side filters supported to help organize mail
- Currently have approximately 3300 users with over 150GB of mail

# POP Services

- POP is still used at Fermilab but the number of active accounts is slowly dwindling
- No new POP accounts are created
- Users are not restricted in the client that is used
- Quotas are strictly enforced and a webmail interface is not available.

# ListServ

- ListServ is used to manage over two thousand mailing lists used at Fermilab by our users and collaborators around the world
- Archived lists have a web interface available to view the archives
- Once created the lists are managed by the list owners
- ListServ processes over 24,000 list messages weekly. These messages are distributed to over 325,000 email addresses

# UNIX/Linux Servers

- No restriction on users receiving mail on their personal UNIX/Linux desktop
- Many users do this and are very happy with managing their own server



# Links

- Dell [www.dell.com](http://www.dell.com)
- Sun [www.sun.com](http://www.sun.com)
- LSI [www.lsillogic.com](http://www.lsillogic.com)
- Microsoft [www.microsoft.com](http://www.microsoft.com)
- Listserv [www.lsoft.com](http://www.lsoft.com)
- Fermi Linux [www-oss.fnal.gov/projects/fermilinux/](http://www-oss.fnal.gov/projects/fermilinux/)
- PostFix [www.postfix.org](http://www.postfix.org)
- SpamAssassin [www.spamassassin.org](http://www.spamassassin.org)
- Sophos [www.sophos.com](http://www.sophos.com)
- Symantec [www.symantec.com](http://www.symantec.com)