Email Services

Securing the eCampus 2009
Central provider of email/calendar

- Chargeback model; no central funding
- 15 subdomains as well as @upenn.edu addresses
- Only faculty, staff, and graduate students
- Zimbra 5.0.x (13,700 users)
- Exchange 2007 (3,100 users)
- About 38% of campus email users
Features

- HA/redundant/geographically distributed
- Domains can be split across services, e.g. staff on Exchange, grad students on Zimbra
- Mobile devices: ActiveSync for both, BlackBerry for Exchange (and piloting under Zimbra)
- AV/AS/Boundary Encryption: Outsourced to MessageLabs
- AuthN: Kerberos for Zimbra, AD for Exchange
- Unified Communications: Voicemail to email
Non-central Services

- Exchange: Annenberg (Center and School), Law, Nursing, Wharton, and various small deployments
- Open Source: Arts and Sciences, Engineering
- Outsourced: Outlook Live, Google, forwards
Message Encryption

- Clients:
  - PGP/GPG not widespread; pockets of users with PGP Desktop, Enigmail, or equivalent depending on policies, IT support
  - More traction for whole disk encryption (campus eval team, campus licensing)
  - Usability and cost are issues in fat clients; web clients should be the focus, but even less optimal solutions
Message Encryption (ctd.)

- **Servers:**
  - Enforce TLS encryption client-to-server
  - Enforce TLS encryption server-to-server (when requested by subdomain owner)
  - Enforce TLS encryption with message hygiene provider
  - Enforce TLS encryption opportunistically
  - New interest in content filtering
Message Hygiene on Campus

- SpamAssassin
- Proofpoint
- Microsoft ForeFront
- MessageLabs
- ... and probably others
This Year’s Central Mail Stats

- 9-15 million inbound messages per month
- 1 million outbound messages per month
- 54% valid
- 45% spam
- 1% virus
MessageLabs Traffic

Total Email Volume

Inbound (140,826,908)
Outbound (11,698,552)

Inbound Summary

Top 5 Viruses Globally
1. Link-Exploit/LinkAli... 4%
2. Link-W32/HackedPacke... 4%
3. Link-W32/HackedPacke... 2%
4. Spy-Agent.bw 2%
5. FakeAlert-AX 2%
6. Other Viruses 86%
MessageLabs Anti-Virus

Virus Volume

Top 5 Inbound Viruses
MessageLabs Anti-Spam

Spam Volume

- Inbound Email (140,826,908)
- Spam (62,896,274)

Spam by Detection Method
- Signaturing system
- DUL
- Skeptic Heuristics
- RBL
- RSS
Campus Stakeholders

- Local Support Providers: Client issues
- Service Providers: Backup/restore, archive for e-discovery, logs
- Information Security: Response, requests, and chain of custody
- Office of General Counsel: E-Discovery, data retention, terms of service
- Office of Audit, Compliance and Privacy: Privacy, sensitive data, and policies
Limitations

- Handhelds - security vs. convenience on 6/4-char PINs; remote management policies; can't keep sensitive data off, but can encrypt in cases

- Retention - Backup software may not make it easy to comply with policies

- Phishing - Users will send passwords, we have tools to automate account locking, but the horse has left the barn
Discussion