



SMTP Virus Filtering @ Texas A&M University

Philip Kizer, CIS



The Distant Past

- In the beginning, CIS was hands-off.
 - ◆ **No central scanning**
 - ◆ **No central servers at all**
- Problems arose with open-relay abuse, complaints out of hand, campus mail hosts getting blocked.



The Past

- Central SMTP relay machines installed.
- TAMU hosts became safe from direct abuse
 - ◆ **No longer possible to abuse TAMU hosts as open-relays.**
 - ◆ **Admins could work on other things than cleaning up after abusers.**
 - ◆ **Opt-out offered (if proven secure), only 12 currently.**



Present

- All mail hosts being hammered by unsolicited mail:
 - ◆ **Mailbombs**
 - ◆ **Viruses**
 - ◆ **SPAM**

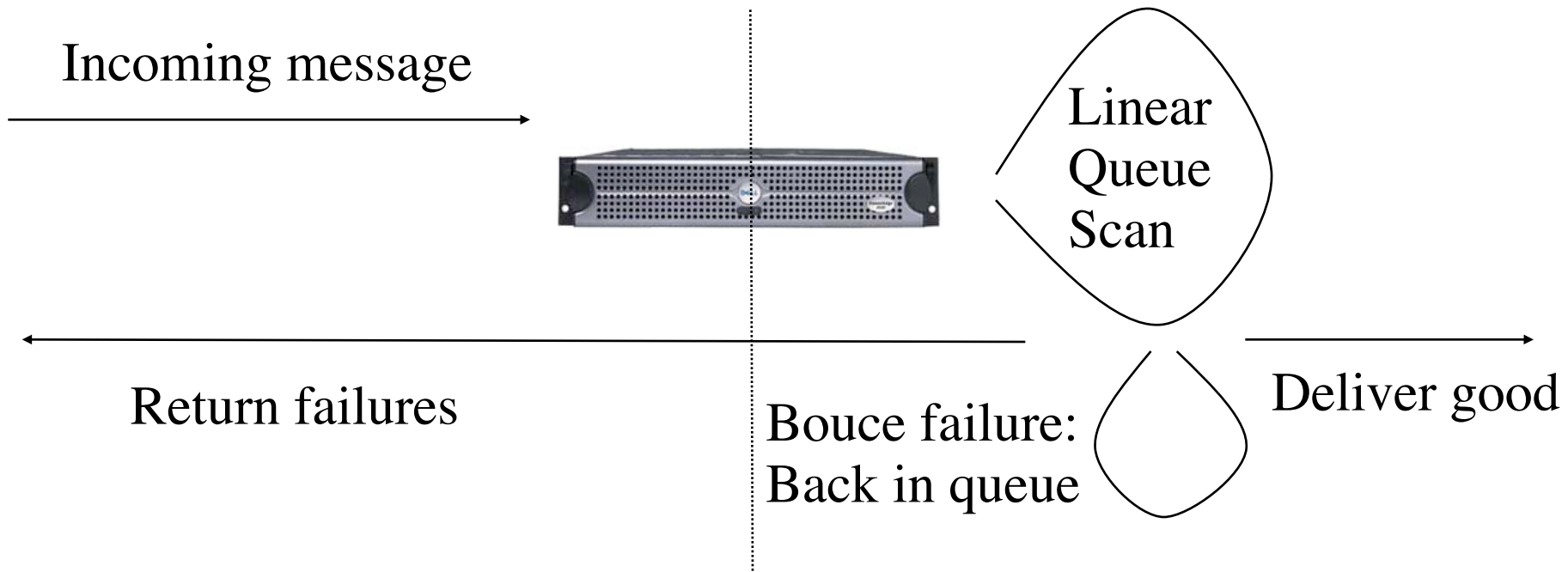


Near-Term Future Plans

- Add Virus Filtering

Scanning methods: queue+scan

- Accept all mail into a special queue
- Virus scan the queue, bounce infected messages
- Deliver clean messages

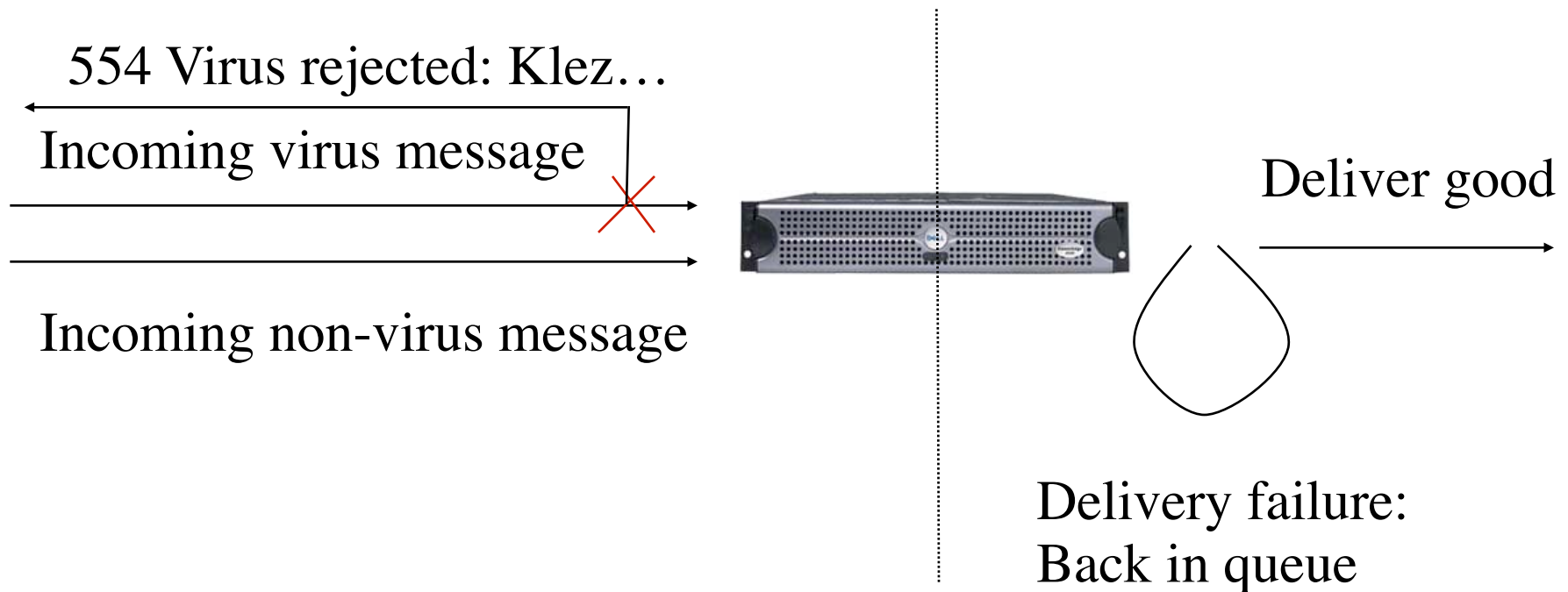


Impact: queue+scan

- Delay between message getting placed in queue and the queue scanner checking the message (queue rescan delay + time to actually scan all messages in queue).
- Faked senders (Klez) that are invalid or undeliverable mail addresses sit in queue for 5 days taking disk space and slowing system.
- Initial attempt to send bounce to bad address delays subsequent messages in the queue.
- We cause faked senders to get messages they did not send.

Scanning methods: scan on input

- Virus messages are never accepted





Impact: scan on input

- Delays message depending on size
- Threaded scanner interacting with the normal sendmail adds a few seconds per message over current (typically sub-second) processing time

Scanning results: Few Products

- Some commercial vendors only offered hardware that was meant to take the place of current smtp-relay machines, causing great increase in complexity.
- Desire a MILTER interface with sendmail:
 - ◆ **Scanning failure allows pass-on-failure**
 - ◆ **Viruses never make it onto campus**
 - ◆ **Remote host responsible for informing of failure**
- PerlMx satisfies the needs.

Additional Future Plans

- Add SPAM scanning:
 - ◆ Perform no blocking based on presumed SPAM content in the beginning, scanning and tagging only.
 - ◆ If we get a good upper-threshold for scanned SPAM values, we will put an opt-in MX server in production that will perform SPAM blocking.
 - ◆ Add a header, those that desire can at least perform their own scanning, including checking if there was an RBL match.

SPAM Tagging Example

- Add SPAM tags as headers, no modifications of existing content.
- Will not modify bodies: can harm MIME structure, or not be viewable.
- Will not modify Subject or other existing headers, which can harm subject sorting/threading of falsely tagged mail.
- X-Perlmx-Spam: Gauge=XXXXXXXXXIIIII, Probability=86%, Report="CTYPE _JUST_HTML, MAY_BE_FORGED, RCVD_IN_BL_SPAMCOP_NET, RCVD_IN_OSIRUSOFT_COM, RCVD_IN_RELAYS_ORDB_ORG, REMOVE_SUBJ, SUBJ_HAS_SPACES, SUBJ_HAS_UNIQ_ID, SUPERLONG_LINE"



Implementing Virus Blocking

- Minimal impact, only blocking technically harmful content.
- Will also allow testing of Spam identification.
- Conservative error conditions.
- Automatically updated VFind signatures multiple times a day.

Questions?

- Security problems and questions:

<security@tamu.edu>

- Join the list:

<listserv@listserv.tamu.edu>

Body: **subscribe ISF Your Name**

<<http://cis.tamu.edu/security/isf/meeting.html>>

