



Greylisting: Keeping the Wolves at Bay

Prepared for the NACS Faculty Advisory Committee
November 28, 2005

by

E. Scott Menter

Director, NACS Infrastructure Services

escott@uci.edu



Greylisting: An Overview

- ◆ It's a protocol test, one which many spammers **fail**
- ◆ Think about what you do when you get a busy signal. Mail servers are supposed to do the same thing!



How it works

Remote Mail Server

I've got email for `dana.roode@uci.edu`
from `scott.menter@gmail.com`

uci.edu Mail Server

I'm busy. Come back later.

🕒 *At least 3 minutes pass....*

I've got email for `dana.roode@uci.edu`
from `scott.menter@gmail.com`

OK, go ahead...





How it works

- ◆ Once accepted, sender/recipient is passed through without delay for **8 days**
 - ◆ Many sites are **never** delayed:
 - ◆ All “.edu” sites
 - ◆ Important government sites, incl. **NSF, NIH**
 - ◆ Significant and well known mail sources
 - ◆ Trouble spots, while we work out the problem
-
-



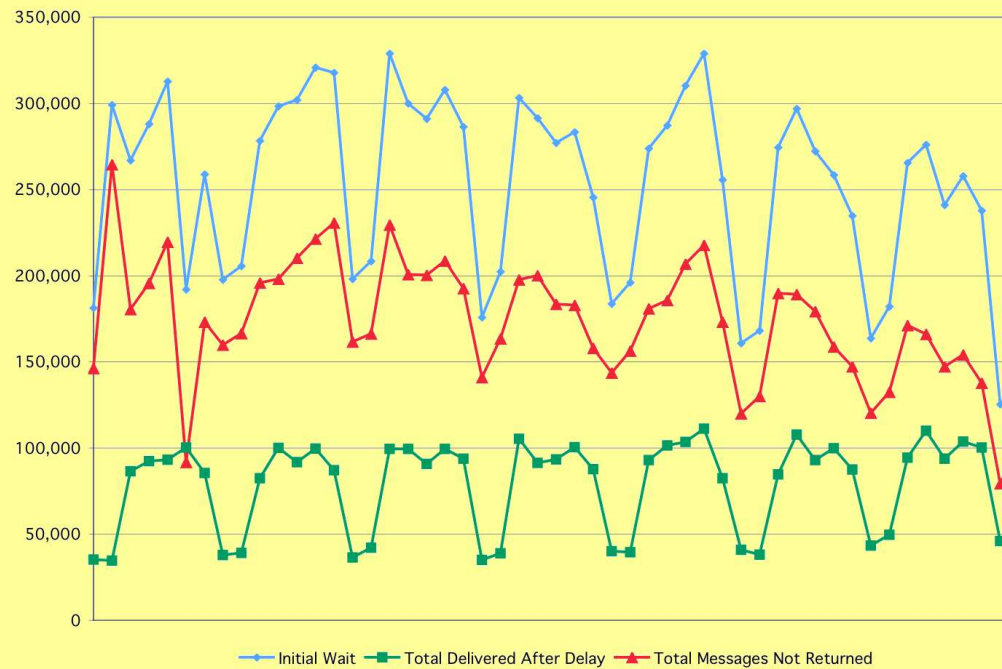
Does it help?

- ◆ Over 150,000 messages are not delivered each day due to greylisting!
- ◆ Failed messages from legitimate mail servers always result in notification to the sender.



Does it help?

Initial Wait, Total Delivered After Delay, and Total Messages Not Returned
Daily totals, 10/1/2005 - 11/20/2005





Does it hurt?

- ◆ Half of all messages are not delayed
 - ◆ Of the remainder, 2/3 are delayed under 45 minutes
 - ◆ Remember, only the **first** message in a “conversation” is delayed... your frequent senders are not delayed at all
-
-



Does it hurt?

- ◆ We process about one complaint per week related to greylisting
 - ◆ Always, **always** due to poor behavior by the sender's ISP
- ◆ We offer opt-out to faculty and staff
 - ◆ Only 4 have taken us up on that so far



What next?

- ◆ Continue our existing anti-spam practices, including greylisting
- ◆ Continue looking for ways to improve accuracy and utility of those practices
- ◆ Continue to seek feedback and input in forums like this one