AutumnTECH Spam Fighting Hardware Appliance: E-mail Flow Chart

Monday, April 11, 2005

Sender

Step 1:
Pass Reject Engine

REJECT MAIL PROCESSING ENGINE
- Greylisting 451 Reject for Infected Proxies
- Reject Dangerous Attachments
- Reject Invalid Hostnames
- Reject Non Fully Qualified Hostnames
- Reject Non Fully Qualified Recipients
- Reject Unknown Domains
- Reject relays.ordb.org RBL Senders
- Reject opm.blitzed.org RBL Senders
- Reject list.dsbl.org RBL Senders
- Reject sbl.spamhaus.org RBL Senders
- Reject cbl.abuseat.org RBL Senders
- Reject dnsbl.us.sorbs.net RBL Senders
- Reject Blacklisted Networks and Netblocks
- Reject Failed Internal LDAP lookup checks
- Reject Sender Policy Framework lookup checks
- Reject if not allowed in appliance firewall access control list

Step 2:
Pass Anti-virus Check

REJECT and ALERT ANTI-VIRUS ENGINE
- Query local ClamAV Anti-virus database for virus signature
- Reject mail if virus detected, alert recipient

Anti-virus database updated three times per day, maintained at www.clamav.net, detects over 34,500 virus, worms, trojans, and phishing scams as of 04/08/2005

Virus Detected

Clean

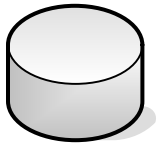
Step 3:
Pass Anti-spam Check

ACCEPTED MAIL PROCESSING SCORING ENGINE
- Whitelisted senders and domains TAG LOW
- Blacklisted senders and domains TAG HIGH
- Bayesian Check ACCUMULATE HIGH TAG
- RBL Sender TAG HIGH
- Static Mail Identity Rules (over 1000 checked) ACCUMULATE HIGH TAG
- Vipul's Razor Internet Message Checksum Lookup TAG HIGH
- SURBL Message Body Domain Lookup TAG HIGH

** VIRUS **
Drop Message
Send Alert

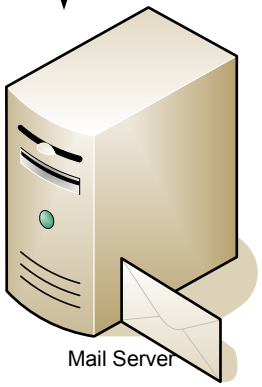
** SPAM **

X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 2.64 (2004-01-11) on jumper.autumntech.com
X-Spam-Level: **********
X-Spam-Status: Yes, hits=17.1 required=5.0 tests=BAYES_99,FORGED_YAHOO_RCVD,
HTML_70_80,HTML_IMAGE_ONLY_04,HTML_MESSAGE,MIME_HTML_ONLY,
MIME_HTML_ONLY_MULTI,MSGID_FROM_MTA_SHORT,RAZOR2_CF_RANGE_51_100,
RAZOR2_CHECK,SPAMCOP_URI_RBL autolearn=no version=2.64
X-Spam-Report:
* 0.1 HTML_MESSAGE BODY: HTML included in message
* 1.1 RAZOR2_CF_RANGE_51_100 BODY: Razor2 gives confidence between 51 and 100 [cf: 100]
* 5.4 BAYES_99 BODY: Bayesian spam probability is 99 to 100% [score: 1.0000]
* 0.1 HTML_70_80 BODY: Message is 70% to 80% HTML
* 0.3 MIME_HTML_ONLY BODY: Message only has text/html MIME parts
* 1.0 HTML_IMAGE_ONLY_04 BODY: HTML: images with 200-400 bytes of words
* 3.0 SPAMCOP_URI_RBL URI's domain appears in spamcop database at sc.surbl.org
[www.rrox.com is blacklisted in URI RBL at sc.surbl.org]
* 1.0 RAZOR2_CHECK Listed in Razor2 (http://razor.sf.net/)
* 3.0 MSGID_FROM_MTA_SHORT Message-Id was added by a relay
* 0.9 FORGED_YAHOO_RCVD 'From' yahoo.com does not match 'Received' headers
* 1.1 MIME_HTML_ONLY_MULTI Multipart message only has text/html MIME parts

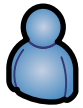


Spam Quarantine

** NOT SPAM **



Mail Server



Recipient

Recipient