



SMTP Spam Scanning @ Texas A&M University

Philip Kizer, CIS



SMTP Relaying

- DNS

```
host.tamu.edu. IN A      10.12.34.56
host.tamu.edu. IN MX    5    host.tamu.edu.
host.tamu.edu. IN MX   90    smtp-relay-4.tamu.edu.
host.tamu.edu. IN MX  100    smtp-relay.tamu.edu.
```

- Firewall

- ◆ **Block SMTP to <host>, connect to next MX**

- Hosts

- ◆ **4 Identical Hosts, locked down and configured all performing SMTP relaying and Virus/Spam scanning, DNS round-robin will become load-balancing**

Whole lotta Spamming

- Networking adage: “Be conservative in what you send and liberal in what you accept” SMTP acceptance has been taken advantage of to the point of abuse.
- Hotmail calculates spam as 80% of their traffic
- What is spam? Can a computer actually identify spam?
- Must become more conservative in acceptance for any reduction.



Types of Unwanted Mail

- Mail bombs
- Technically incorrect connections
- Technically incorrect content (headers)
- Undesired/unsolicited content (Spam)



Mail bombs

- One or more hosts sending to large number of local recipients or stuck in a mail loop
- One host making multiple simultaneous connections to a single local server (taking all available connection slots)

Technically incorrect connections

- Typically 2 causes, results are the same:
 - ◆ **Hosts/systems that are simply misconfigured**
 - ◆ **Spam sources that want to spew and not receive**
- Hosts without proper DNS
 - ◆ **Unable to send responses**
 - ◆ **Most MTAs will temporarily reject these by default**
- Not compliant with RFC1123, etc.
 - ◆ **Unable to send bounces**
 - ◆ **<http://www.rfc-ignorant.org/>**

Technically incorrect content

- Two causes here, too:
 - ◆ **Misconfigured clients**
 - ◆ **Intentional incorrect settings to hide or limit replies**
- From: To: or Message-Id: headers not RFC2822-compliant
 - ◆ **From: Missing @host or obviously invalid like <subscriber@smtp-relay.tamu.edu>**
 - ◆ **To: Missing @host or invalid as above, or not a distribution list format “To: User List;”**
 - ◆ **Message-Id: not of the form <local-part@host-part>**



Undesired or Unsolicited Content (Spam)

- Completely subjective, only the end recipient can tell you if a message was spam
- Even those that might say yes to blocking spam tend to have different criteria for determining what is spam

Comments from ISF:

- “I usually have about a 1% false positive...cannot consider [blocking]...unless I can review”
- “TAMU users forward possible spam mail for...inclusion”
- “spammers are looking for valid e-mail addresses...Couldn't we take like...75...up to just delete”
- “legitimate "blanket" emails from vendors...that I think should be allowed through”
- “I also believe the University should filter spam also. Neither of these should be optional.”
- Requests for everything to be an option: Virus, Spam content, RBL, etc.
- A suggestion to start our own registry of known spammers...

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"

Web pages and Spam Tags

- Example from above:

- ◆ **X-PerImx-Spam: Gauge=XXXXXXXXXIIIIII, 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"**

Suggestions:

- There is **no** way to remain completely spam-free
- Best efforts to stay off the spam lists:
 - ◆ **Do not give out your email address indiscriminately to web forms**
 - ◆ **Never respond to spam you receive**
 - ◆ **If you own a mailing list, make sure the subscribers cannot be retrieved (difficult), verify subscribers**
 - ◆ **Beware web publishing of your address**
- Help us provide filtering examples for others:
 - ◆ **(outlook, groupwise, procmail, etc)**

Questions?

- Security problems and questions:

<security@tamu.edu>

- Windows Virus Scanners:

<https://software.tamu.edu/>

- Join the list:

<listserv@listserv.tamu.edu>

Body: **subscribe ISF Your Name**

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

