Bounce Address Tag Validation (BATV)

“Was use of the bounce address authorized?”

D. Crocker
Brandenburg InternetWorking
mipassoc.org/batv
03/08/05 13:11
# Basic Email Roles

<table>
<thead>
<tr>
<th>Who</th>
<th>Specified in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator (author)</td>
<td>Content – From/Resent-From</td>
</tr>
<tr>
<td>Submitter into transfer service</td>
<td>Content – Sender/Resent-Sender</td>
</tr>
<tr>
<td>Return address (bounces)</td>
<td>Envelope – Mail-From</td>
</tr>
<tr>
<td></td>
<td>Content – Return-Path</td>
</tr>
<tr>
<td>Sending Relay</td>
<td>Envelope – HELO/EHLO</td>
</tr>
<tr>
<td></td>
<td>Content – Received header</td>
</tr>
<tr>
<td>Receiving Relay</td>
<td>Content – Received header</td>
</tr>
</tbody>
</table>
Bounce Addresses Abuse

- Redirecting flood of bounces
  - Spam sends to many invalid addresses, thereby causing masses of bounces.
  - Spammers specify stray bounce addresses – like yours -- just to get the traffic off the sending service

- Backdoor trojan
  - Bounce message, itself, might contain dangerous content

- Denial of service
  - The flood of messages can cripple the bounce receiving site
Bounce Address Validation Goals

- **Bounce recipient delivery agent**
  - Should I deliver this bounce?

- **Bounce originator**
  - Should I create this bounce?

- **And by the way…**
  - If the bounce address is invalid, the entire message is probably invalid
  - If we can detect forged mail, we do not need to worry about its bounce address
**BATV**

- Sign envelope **Mail-From** address
  - Protect against simple bounce address forgery
  - Possibly protect against unauthorized re-use of signature

- Submission Agent adds sig to bounce address

  MAIL FROM mailbox@domain ⇒
  MAIL FROM **sig-scheme=**mailbox/sig-data@domain

- Multiple signature schemes
  - **Symmetric** – can only be validated by signer’s admin
  - **Public** – can be validated by relays on original path
A Symmetric BATV Signature

- Originating site uses any signing scheme
- BATV spec provides a simple version

\[
joe-user@example.com \Rightarrow prvs=joe-user/tag-val@example.com
\]

\[
tag-val = \text{Encryption of (day address will expire, original mailbox@domain)}
\]
Public BATV Signature

- Same style as for symmetric key approach
  - Except that originating site uses symmetric key and the evaluating site must obtain the public key

- Public key distribution is the core difficulty
  - Therefore, piggyback the effort on an existing message encryption effort, like DomainKeys and Identified Internet Mail
  - Unfortunately, no existing public key-based message signing effort has widespread support… yet
Several rounds of specification and open comment

Now recruiting field experience

Plan to pursue IETF standardization
To follow-up…

- Mailing list
  http://mipassoc.org/mailman/listinfo/ietf-clear

- BATV specification
  http://ietf.org/internet-drafts/…
  * Bounce Address Tag Validation (BATV)
    draft-levine-mass-batv-00.txt

- Internet mail architecture
  http://bbiw.net/current.html#email
  * draft-crocker-email-arch-03.txt