MIPA

Bounce Address Tag Validation (BATV)

"Was use of the bounce address authorized?"

D. Crocker

Brandenburg InternetWorking

mipassoc.org/batv

11/26/2004 1:39 PM

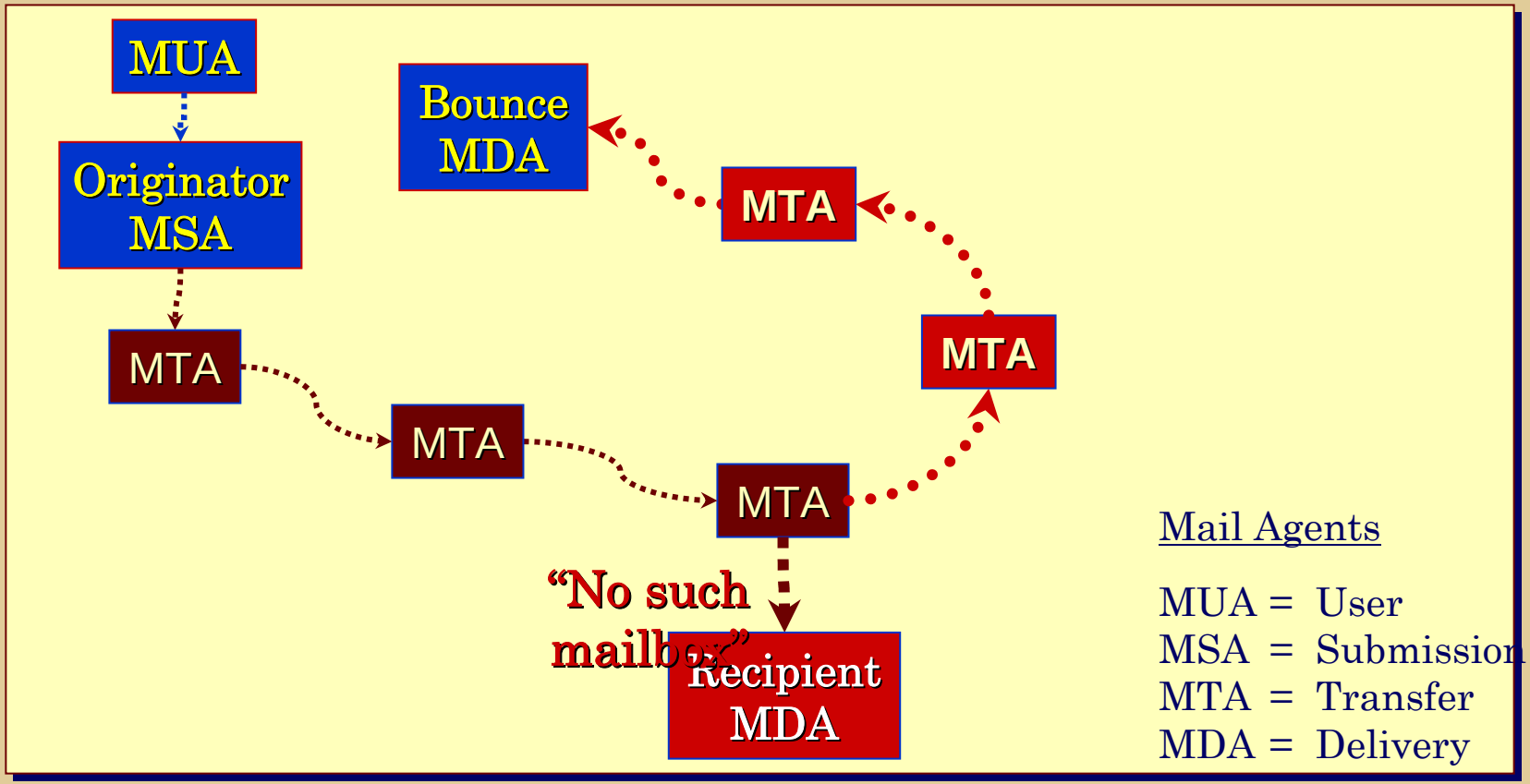
Basic Email Roles

Who	Specified in
Originator (author)	Content **`From`** or **`Resent-From`**
Submitter into transfer service	Content **`Sender`** or **`Resent-Sender`**
Return address (bounces)	Envelope **`Mail-From; and`** Content **`Return-Path`**
Sending Relay	Envelope **`HELO`** or **`EHLO;`** and Content **`Received`** header
Receiving Relay	Content **`Received`** header

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

Original Path and Bounce Path



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 forgery
  - Possibly protect against unauthorized re-use of signature
- Submission Agent adds signature to bounce address

  `MAIL FROM mailbox@domain` ⇒

  `MAIL FROM sig-scheme=mailbox/sig-data@domain`
- Multiple signature schemes

  Private – can only be validated by signer's admin

  Public – can be validated by relays on original path

A Private BATV Signature

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

  prvs=joe-user/tag-val@example.com

  tag-type = “prvs"

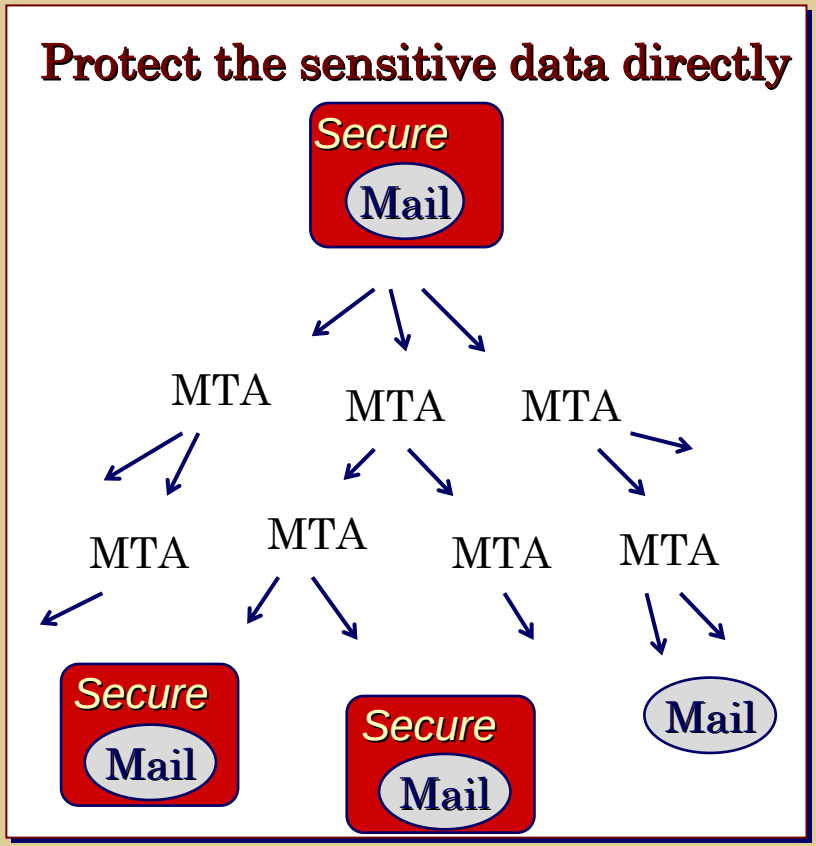
  tag-val = Encryption of
  (day address will expire,
  original mailbox@domain)

Public BATV Signature

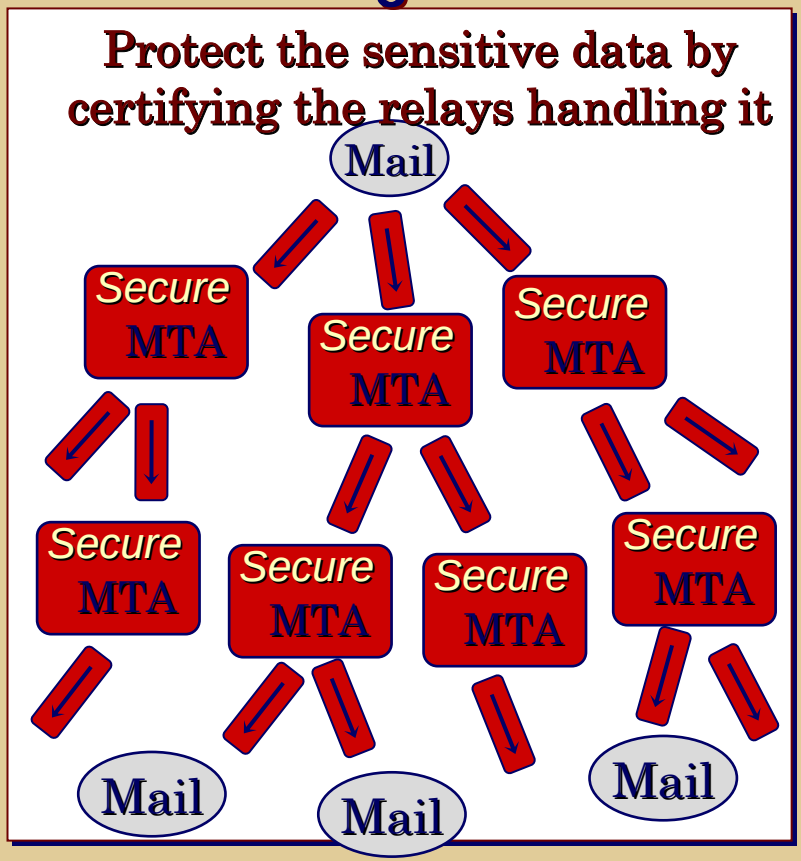
- Same style as for private key approach
  - Except that originating site uses private key and the evaluating site must obtain the public key
- Public key distribution is the core difficulty
  - Therefore, piggyback the effort on an existing message encryption effort, like DomainKeys and Identified Internet Mail
  - Unfortunately, no existing public key-based message signing effort has widespread support… yet

Object vs. Channel

BATV



Path Registration



Status

- Several rounds of specification and open comment
- Beginning to solicit experimental implemtations
- 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

  - draft-crocker-email-arch-01.txt