Message Authentication Signature Standards (MASS) BOF

Jim Fenton <fenton@cisco.com>

Nathaniel Borenstein <nsb@guppylake.com>

Agenda

- Introductions and Agenda Bashing (10 min)
  - Scribe??
- Overview of existing signing proposals: (5 min each)
  - Identified Internet Mail
  - DomainKeys
  - E-mail Postmarks
  - Entity-to-entity S/MIME
  - MTA Signatures
  - Bounce Address Tag Validation
- Proposed WG goals/non-goals (15 min)
- Proposed WG charter (15 min)
- Proposed WG Deliverables/Schedule (15 min)
- Discussion /Summary (30 min)

WG Goals

- Facilitate automated signing of outgoing messages by any SMTP-initiating entity
- Provide a reliable basis for classifying messages based on sender address and message signature
- Minimize required impact on low-end clients
- Minimize computational and transactional overhead for high-volume email servers
- Preserve anonymity if desired by the sender
- Don’t break e-mail

WG non-goals

- Accreditation/reputation
- Force server or client “flag day”
- Determine the intent of an e-mail message
  - Infer anything other than the identity
- Non-repudiation
- Message encryption
- Break e-mail

MASS relationship to MARID

- MARID:
  - Authorization based on IP address
  - Authorization records stored in DNS
  - Cryptographic approaches out-of-scope
- MASS:
  - Message authentication based on cryptographic signature
  - Authorization of key (and often key itself)
    - May be stored in DNS
    - May be a separate server

Potential commonalities between MASS and MARID

- Definition of Purportedly Responsible Address (PRA)
- Message marking to indicate successful/unsuccessful verification
- Eventual use of accreditation infrastructure
  - Although what's being accredited may differ

Representative proposals

- **DomainKeys**
  - draft-delany-domainkeys-core-00
- **Identified Internet Mail**
  - draft-fenton-identified-mail-00
- **E-mail Postmarks**
  - http://www.lessspam.org/EmailPostmarks.pdf
- **Entity-to-entity S/MIME**
  - draft-hallambaker-entity-00
- **MTA Signatures**
  - http://www.elan.net/~william/asrg/mta_signatures.html
- **Bounce Address Tag Validation**
  - http://brandenburg.com/specifications/draft-crocker-marid-batv-00-06dc.html

DomainKeys

See:

DK-ietf60.pdf

Identified Internet Mail

See:

IIM-MASS.pdf

E-mail Postmarks

See:

EMailPostmarks040805.pdf

Entity-to-Entity S/MIME

See:

Entity-to-Entity.pdf

MTA Signatures

See:

IETF60-MTA_Signatures-Brief.pdf

Bounce Address Tag Validation

See:

Strivers-BATV.pdf

Issues for WG to resolve

- Signature encapsulation
  - Signatures in headers
  - S/MIME
- Key management, revocation, duration
- Canonicalization
  - What's required to avoid signature breakage?
  - Treatment of headers, character sets
- Behavior through mailing lists

WG Name?

- MASS
  - Message Authentication Signature Standards
- STRIVERS
  - Signatures for Transport Recognition of Imposture in Viral Email and Repugnant Spam
- HUM??

Charter

- Message recipients need the ability to reliably determine the source of incoming messages as a tool in countering spam and phishing attacks, which are frequently characterized by spoofed return addresses. One approach to this problem is the inclusion of digital signatures in email messages. Past attempts at widespread deployment of digital signatures have met only very limited adoption, and only a small fraction of today's email messages are cryptographically authenticated in any way.
- Several proposals have recently been published for simple and automatic mechanisms by which outgoing messages may offer limited proof of potentially-verifiable identity. Although there are already more than a few mechanisms for attaching a digital signature to an email message, none meet the particular set of constraints for this problem. The ideal signing mechanism for this problem would:
  - Facilitate automated signing of outgoing messages by any SMTP-initiating entity
  - Minimize computational and transactional overhead for high-volume email servers
  - Permit a high degree of anonymity when desired by the sender

Deliverables

- In conjunction with responsible WGs, extensions (where required) to SMTP, RFC 2822, and/or MIME that will enable any SMTP-sending entity to:
  - Convey the fact that a cryptographic signature is associated with the message being delivered
  - Convey the identity and public key of the signing entity
  - Identify the precise message contents being signed (notably which headers)
  - Deliver the signature along with the message
- A mechanism by which a message recipient may verify the public key of an SMTP sender

Strawman Timeline

- DONE Establishment of mailing list
- Aug 04 BOF meeting at San Diego IETF. Selection of WG leaders
- Aug-Oct 04 Requirements formulation
- Oct 04 Interim meeting. Finalization of requirements
- Nov 04 Publish signature syntax proposals for discussion
- Nov 04 WG meeting at Washington IETF
- Mar 05 Publish first drafts of "consensus" documents
- Mar 05 WG meeting at IETF conference
- Apr 05 Publish more drafts of "consensus" documents
- Jun 05 Publish more drafts of "consensus" documents WG Last Call
- Jul 05 WG meeting at IETF conference
- Aug 05 Publication of RFC(s) as Proposed Standard.
- Aug 06 Publication of RFC(s) as Draft Standard.
- Aug 07 Publication of RFC(s) as Full Standard.

Mailing List

- Mailing list: <ietf-mailsig@imc.org>
  - Archive at http://www.imc.org/ietf-mailsig/
  - Subscribe in the “usual way”