E-Mail Postmarks

Jim Lyon
Microsoft Corporation
5 August 2004

Goal

- Attach authenticatable information to E-Mail messages.
  - Prove that an E-mail was transmitted by a specific domain.
    - (same goal as Domain Keys, Identified EMail, ...)
  - Other uses possible.

Observations

- Digital Signatures rely on bit-for-bit replication of email.
- Some existing MTA’s don’t just transport, they also change headers and bodies.

Header Munging

- Headers get reordered.
- Headers get removed.
- Headers get changed:
  - Whitespace and comments get lost.
  - Unfolding / Refolding.
  - Ambiguous folding.
  - Character decoding and re-encoding.

Body Munging

- End-of-line whitespace gets added / removed.
- Transfer decoding and re-encoding.
- Loss of MIME prolog / epilog.
- Rewriting MIME multipart delimiters.
- MIME body part elision.
- Content format conversion.
- HTML sanitization.
- Add tag lines to content.

Observation – 2

- MTA/s know not to munge e-mail when Content-Type=multipart/signed.
  - So, make domain signing operation use S/MIME.
    Find an innocuous place in S/MIME for domain signature.
    - But not a traditional signature.

S/MIME Signatures

- SignedData ::= SEQUENCE {
  version CMSVersion,
  digestAlgorithms DigestAlgorithmIdentifiers,
  encapContentInfo EncapsulatedContentInfo,
  certificates CertificateSet
  crls CertificateRevocationLists
  signerInfos SignerInfos }
- SignerInfos ::= SET OF SignerInfo
- SignerInfo ::= SEQUENCE {
  version CMSVersion,
  sid SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttrs SignedAttributes
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature SignatureValue,
  unsignedAttrs UnsignedAttributes }

S/MIME Signatures

- CertificateSet ::= SET OF CertificateChoices

- CertificateChoice ::= CHOICE {

```
    Certificate              Certificate                  -- X.509
    extendedCertificate      [0] ExtendedCertificate,     -- Obsolete
    attrCert                 [1] AttributeCertificate,    -- X.509, X9.57
    signerInfos              [42] IMPLICIT SignerInfos -- new }
```

- Existing code ignores certificates that they don’t understand.
- So, new “certificate” type is domain signer info.

Summary

- Similar goals to IIM and DK
- Use S/MIME to get past MTA behavior
- Leverage existing S/MIME extensibility

- More info:

  http://www.lessspam.org/EmailPostmarks.pdf