Protecting message header, again

Alexey Melnikov <alexey.melnikov@isode.com>

Problem statement

- Most S/MIME implementations don’t protect (encrypt and/or sign) message header.
- Subject, Date (,From, To, etc) header fields can possibly contain sensitive information that needs hiding, integrity protection or both.
- RFC 5751/draft-ietf-lamps-rfc5751-bis say that header protection can be done by wrapping inner message by “Content-Type: message/rfc822” wrapper. So true copies of Subject, Date, etc can be included in the inner message.

Example message demonstrating how this is supposed to work (1 of 2)

Outer header:

date: Tue, 22 May 2018 11:23:44 +0100 (GMT Daylight Time)

from: alexey.melnikov@isode.com

subject: Fake subject

to: test@example.com

x-mailer: Isode Harrier Web Server

MIME-Version: 1.0

content-type: multipart/signed; micalg=sha1;
 protocol="application/pkcs7-signature";
 boundary=.057c5ca4-5d7e-47c9-ab72-c32f0fb5a736

This is a multipart message in MIME format.

--.057c5ca4-5d7e-47c9-ab72-c32f0fb5a736

Example message demonstrating how this is supposed to work (2 of 2)

Inner header and message:

Content-Type: message/rfc822; forwarded=no

content-type: text/plain; charset=us-ascii; delsp=yes; format=flowed

date: Tue, 22 May 2018 11:23:44 +0100 (GMT Daylight Time)

from: alexey.melnikov@isode.com

mime-version: 1.0

subject: Signed and Protected, BCCed to self

to: test@example.com

x-mailer: Isode Harrier Web Server

Keep Calm!

Problems

- Minor problem: this is ambiguous, because there is no way of distinguishing header protection from a forwarded message
- Major problem: no S/MIME implementation other than Isode Harrier seems to implement header protection
  - Please correct me if I am wrong!

Common email clients display messages with header protection as forwarded messages:

This is ugly/confusing to users

Ways to fix this

1. “Memory hole” approach: https://github.com/autocrypt/memoryhole

2. RFC 7508 approach: new ASN.1 encoded attribute that contains individual header fields to be protected is included in the protected CMS.

3. Nothing is wrong with the current RFC, make clients fix header protection

Ways to fix this

#1: “Memory hole”: what some PGPMime clients are doing. Instead of wrap the message inside message/rfc822, just include copy of header fields that need protecting alongside the Content-Type header field:

content-type: text/plain; charset=us-ascii; delsp=yes; format=flowed

date: Tue, 22 May 2018 11:23:44 +0100 (GMT Daylight Time)

from: alexey.melnikov@isode.com

subject: Signed and Protected, BCCed to self

to: test@example.com

Keep Calm!

Ways to fix this

#1: What some PGPMime clients are doing: don't wrap the message inside message/rfc822, just include copy of header fields that need protecting alongside Content-Type header field

- Pros: this is less ugly (when displaying) in existing clients that don't do anything special about header protection. No need to change them.
- Cons: RFC 5751 needs to be updated

Ways to fix this

#2: RFC 7508 approach

- Pros/Cons: As for #1

Ways to fix this

#3: No changes to the RFC 5751

- Pros/Cons: The reverse of #1/2

What to do next?

- Who wants to help to fix the problem?
- Opinions about the best option?