Protecting message header

Alexey Melnikov <alexey.melnikov@isode.com>

Problem statement

- Most S/MIME implementations don’t protect (encrypt and/or sign) message header
- Subject, Date header fields can possibly contain sensitive information that needs hiding from unintended recipients, integrity protecting or both
- RFC 5751/draft-ietf-lamps-rfc5751-bis-12 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. But this is not followed by most common implementation
- OpenPGP has a similar need

Problems with what specified in draft-ietf-lamps-rfc5751-bis-12

- 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

- Implementors need more information about what put in the “inner” (protected) header, what put in the “outer” and how to display information from both, especially if it is in conflict

- Clients that don’t support what is in the RFC display a nested message, which is confusing to users (and sometimes not viewable in badly written clients)

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

    - *<**SHOW AN EXAMPLE**>*

    - 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 XXXX needs to be updated

2. Reach out to vendors of existing S/MIME clients to really implement header protection as specified in RFCs

    - Pros/Cons: the reverse of the above

How do we fix that?

- Briefly discuss requirements on the solution
  - Don’t need to publish this as an RFC
- Do some testing of existing implementations of both approaches and see how legacy S/MIME clients handle 2 proposals
- Do interop before or during Montreal IETF in summer 2019?
- Pick one solution
- Concentrate on instructions for minimising unprotected header fields
- Easy ;-) !