Header Protection: WGLC

IETF 116
LAMPS

Bernie Hoeneisen
Alexey Melnikov
Daniel Kahn Gillmor

draft-lamps-header-protection

- **`hcp_minimal`** is recommended default HCP
- MUST be able to generate and interpret Injected Headers
  - MAY include “Legacy Display” elements in main body
- MAY generate Wrapped Messages, MUST be able to interpret
  - Changed from **`forwarded=no`** to **`protected-headers=wrapped`** (with recommendation for **`Content-Disposition: inline`**)
- **`HP-Removed`** and **`HP-Obscured`** headers enable the recipient to reason about sender’s HCP (intended confidentiality of each field)

Two Schemes (A)

- Injected Headers:
  - 100% legacy-compatible for signed-only messages and encrypted messages with cleartext user-facing headers
  - For an encrypted message with an obscured user-facing header sent to decryption-capable legacy clients: decorative “Legacy Display” elements added to main message body parts.
  - Can generate without risk

Two Schemes (B)

- Wrapped Message
  - More similar to older, unimplemented S/MIME 3.1
  - Interop issues with legacy clients
  - Some attempts to work around this (**`protected-headers=wrapped`**, **`Content-Disposition: inline`**)
  - Should be able to handle for existing messages

Header Confidentiality Policy

- Encrypted messages: Which headers should be hidden?
- HCP is an abstraction
  - **`hcp_null`**: hide nothing
  - **`hcp_minimal`**: only hides the **`Subject`** header
  - Future work…

Reasoning about messages

- Guidance about handling on receipt
- Mechanism for thinking about sender's HCP (**`HP-Obscured`** and **`HP-Removed`**)
- Guidance for replying safely to encrypted messages

Retitling

- From “Header Protection for S/MIME” to “Header Protection for Cryptographically Protected E-mail”
- The document still explicitly focuses on S/MIME (e.g. test vectors), but none of the mechanisms depend on S/MIME (as opposed to PGP/MIME).

Evolution (future work)

- When can a MUA stop adding Legacy Display elements?
- When can a MUA indicate a warning for cryptographic messages whose headers are *not* protected?
- How should a MUA indicate to the user that some headers have higher confidentiality than others?
- Additional nuance (e.g. Bcc) not specifically header-related mostly in **`draft-ietf-lamps-e2e-mail-guidance`**
- Future versions of HCP?

WGLC?

- Authors think this is ready for Working Group Last Call