Guidance on End-to-end E-mail Security and Header Protection

Daniel Kahn Gillmor <dkg@fifthhorseman.net>

IETF 119

LAMPS session

March 2024

draft-ietf-lamps-header-protection-20

- Substantive Changes since IETF 118 (draft -17):
  - Only US-ASCII as modified output of HCP
  - Request HCP registry from IANA
  - Drop IANA nudge about Content-Type parameters registry
  - Expand Security Considerations references
  - Tighten up SHOULDs/MUSTs for conformant MUAs
  - Now formally Updates 8551
  - Normalize pseudocode variable names and text (no algorithmic changes)
  - Still in MISREF state, waiting on **`e2e-mail-guidance`**

Designated Expert Qs for Header Protection

- HP-Removed and HP-Obscured contain header field names in their values. Header field names are case-insensitive by definition, but header field values are not necessarily.
- Do we need to add any explicit guidance about case-insensitivity for HP-Removed and HP-Obscured?

draft-ietf-lamps-e2e-mail-guidance-16

- IESG, SEC AD, directorate, Last Call
- Changes since IETF 118 (draft -12):
  - Clarify MUA categories (“conformant”, “legacy”, “non-cryptographic”)
  - Tighten up MUSTs for conformant MUAs
  - Explicitly recommend encrypting drafts
  - Guidance on receiving “Weak Encryption”
  - Three states for sending (normal, signed, signed+encrypted), four for receiving (since sigs might fail)

- More Future Work:
  - Webmail
  - Mailing lists
  - Human-readable names

e2e-mail-guidance next steps

- Cleared IESG review
- Ready for RFC editor, unless we want to ask for BCP status instead of Informational

Requests to WG

Feedback on Expert Q for Header-protection?

e2e-mail-guidance: BCP?

“Future Work” section of e2e-mail-guidance is calling...