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

Daniel Kahn Gillmor <dkg@fifthhorseman.net>  
Bernie Hoeneisen  
Alexey Melnikov  
IETF 120  
LAMPS session  
July 2024
Header Protection draft-23 (1/2)

Substantive changes since IETF 119 (draft -20)...

- Major document reorganization for readability
- HP-Outer replaces HP-Removed and HP-Obscured
- hp= parameter for Content-Type indicates sender’s cryptographic intent ("clear" vs. "cipher")
- Safe handling of replies and forwards
- Explicit algorithm for computing per-header protection status
Header Protection draft-23 (2/2)

Substantive changes since IETF 119 (draft -20) (...continued)

- Rename hcp_null to hcp_no_confidentiality
- Rename hcp_minimal to hcp_baseline, and have it also remove Keywords and Comments
- Replace hcp_strong with hcp_shy (obscures display-names and TZ info, no threading issues)
- Remove Wrapped Message, rename “Injected Headers” to “Header Protection”
- Test vectors: show unwrapped forms of messages
- Offer guidance for dealing with RFC8551HP messages
- Address risk of From header spoofing
Simplification: One Scheme

• Only one scheme, now just called “Header Protection” (was “Injected Headers”)

• “Wrapped Message” was removed: no one implements it, it has usability issues with legacy MUAs.

• Draft is simpler, shorter.
HP-Outer

- Goal: represent the sender’s initial intent of what was sent on the outside of an encrypted message.
- HP-Removed and HP-Obscured could not clearly represent distinct changes to multiple headers of the same name.
- HP-Outer is simpler!
Header Confidentiality Policies

- `hcp_baseline` replaces `hcp_minimal`: also removes Comments and Keywords
- `hcp_shy` replaces `hcp_strong`: more subtle, removes display-names and TZ info, less likely to cause deliverability and rendering issues
Risk: “From” Spoofing

• If the MUA always renders the protected From...
• And the user depends on the MTA to ensure that “From” is authentic (e.g. DKIM+SPF+DMARC or some other policy)...
• Then the sender could bypass the MTA-based quarantine!
Guidance to avoid “From” spoofing

- Valid e2e cert for protected From signed message is OK to render, regardless of MTA filtering. **e2e verification is sufficient.**

- Invalid cert, cert with address that doesn’t match, or invalid signature: **show the “outside” From** (the one that the MTA used for filtering).

  *(highlighted parts are contentious, see #87)*

- Document how to match addr-specs.
• Remains where it was, waiting on Header Protection
Requests to WG

Feedback on guidance for spoofing risks on From

Final WGLC on Header Protection