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

Daniel Kahn Gillmor <dkg@fifthhorseman.net>
Bernie Hoeneisen
Alexey Melnikov

IETF 121
LAMPS session
November 2024

Header Protection draft-24 (1/2)

- With the IESG!

  Substantive changes since IETF 120 (draft -23)...
- Deal with `From` spoofing risk:
  - If (no valid signature and

    inner and outer `From:` differ), then
    - Render outer `From:` and warn (like “spam”)

Header Protection draft-24 (2/2)

Substantive changes since IETF 120 (draft -23) (...continued)

- Add test vectors to show historical 8551HP variants
- Clarify PEF-2 and `draft-autocrypt` commentary

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) and warn (similar to potential spam warning).
- §4.4.5 Documents how to match addr-specs.

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

- Remains with RFC-editor, waiting on Header Protection

Requests to WG

Encourage the IESG to complete the review?