Guidance on End-to-end E-mail Security

Daniel Kahn Gillmor <dkg@fifthhorseman.net>

IETF 116

LAMPS session

2023-03-29

draft-ietf-lamps-e2e-mail-guidance-05

- Recent changes (in draft -05):
  - Guidance about Bcc and encrypted e-mail
  - Risks of a transparent proxy implementation architecture
- In git (not yet in a draft):
  - Expand proxy warnings to comparable APIs
  - Reference JMAP work

Document Status

- Some useful feedback from Bernie Hoeneisen and Alexey Melnikov
- Not much input from other implementers
- Risks being a source of a MISREF hold on Header Protection draft

Proposed path forward

- Recommend doing Header Protection
- Guidance will need to evolve, but we need a stable reference for current useful insights (in particular, to unblock HP MISREF)
- Tighten content, aim for publication (ask for WGLC at or before IETF 117)

How do we get there?

- Drop “test vectors” TODO (other drafts have test vectors already, this can be done separately)
- Move most certificate management guidance (all current TODOs) to “out of scope/future work” section
- Resolve remaining FIXMEs (some by moving to future work, others by providing simple text)

Outstanding questions

- certificate management guidance (peer certs, own certs)
- indexing and search of encrypted messages
- managing access to cryptographic secret keys that require user interaction
- secure deletion
- storage of composed/sent messages
- cached signature validation
- aggregated cryptographic status of threads/conversations
- draft messages
- copies to the Sent folder

Request to WG

Please give feedback!
Provide text for specific topics
Share your hard-earned insights
Point other MUA developers to the draft