REQUIRETLS
draft-fenton-smtp-require-tls-03

Jim Fenton

IETF 99

Review: Problem statement

- Senders have no idea whether transmission will be TLS protected
  - STARTTLS is opportunistic; delivery takes priority
  - TLS certificate verification typically ignored
  - But this is often what you want
- Some senders want to prioritize security over delivery for (at least) some messages
  - Sensitive message content
  - Sender or recipient in sensitive location

Review: Goals

- Allow senders to specify when envelope and headers require protection
- Fine-grained
  - Don't affect messages not specifying REQUIRETLS
- Some control over certificate verification
  - Bad actors with root certs
  - Unknown trust by intermediate MTAs
- MTA <-> MTA only
  - But last hop could require secure retrieval?

Review: Approach

- Negotiate REQUIRETLS service extension
- Send messages with specific TLS requirements using REQUIRETLS option on MAIL FROM:
  - Can require use of TLS, optional cert verification
  - Can also NOT require TLS, for “priority” messages when SMTP TLS policy exists
- REQUIRETLS requirements follow the message
- No policy discovery needed!

What's new?

- Not much, due to other commitments
  - But this is changing
- Still consider this to solve an important problem

WG Adoption?

- REQUIRETLS solves a different problem from MTA-STS
  - Sender-side requirement
  - Finer grained (per-message)
- Have two implementations
  - Exim and MDaemon
- Consistent with WG goal “to increase the security of transmissions over the Internet”