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

Jim Fenton
IETF 98
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?

• Internet Draft revised 13 February
  – Thanks for the comments received
  – More on the new draft to come...

• Two MTA prototype implementations
  – Exim (Jeremy Harris)
  – MDaemon (Arvel Hathcock)
What’s new in -03

• REQUIRETLS=NO
  – Suggested by Viktor Dukhovni as “MAY TLS”
  – Overrides policy mechanisms (DANE, MTA-STS) for “high priority” messages

• Additional bounce guidance
  – Issues with handling of bounce messages when return path doesn’t meet specified REQUIRETLS
Some Issues

• Advertising REQUIRETLS in EHLO
  – Advertise prior to negotiating STARTTLS? Can’t be used until STARTTLS is negotiated.
  – May be moot issue with REQUIRETLS=NO

• REQUIRETLS DANE and CHAIN options
  – Over-engineered (unlikely to be used)?
  – Needed for state-level attackers with ability to sign certificates?
Some More Issues

• REQUIRETLS DNSSEC option
  – Usual skepticism on DNSSEC deployment
  – Spoofing MX response overrides cert scope

• Bounce Messages
  – May be lost if return path doesn’t have equivalent REQUIRETLS capabilities
  – Is there a way to send a bounce that doesn’t spill too much information?
Wishes

• More comments/review
  – Hard to gauge rough consensus with 2 people
• WG adoption
  – Some degree of maturity as gauged by interoperable implementations
• Others who want to try it out
• Questions?