Review: Problem statement

• Senders (including users) 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?

• Now a WG draft!
• Working with author of ‘swaks’ tool to use it for testing support
• Still two implementations (Exim and MDaemon) [not new]
Issues: REQUIRETLS=NO

• Pro:
  – Increases utility by adding mechanism for sending high priority messages regardless of MTA-STS

• Con:
  – Fragile: Also has to deliver to non-REQUIRETLS MTAs, so message can easily lose NO option
  – Adds implementation complexity: works in opposite direction of other REQUIRETLS options
Issue: Option granularity

• Basic STARTTLS+REQUIRETLS requirement
• Option to require DNSSEC MX lookup
• Option to constrain type of cert verification
  – X.509 trust chain
  – Use of DANE certificates
• Optional constraints on crypto characteristics
  – Minimum TLS version
  – Cipher choices, etc.
• Options can greatly complicate implementation but make protocol robust against additional attackers
MORE REVIEWS PLEASE!