What’s new?

• Now two separate mechanisms:
  – REQUIRETLS SMTP option to require transport security when transmitting a given message
  – RequireTLS: NO header field to override policy-based requirements to use TLS
RequireTLS: NO header field

• When present, requests that MTA ignore policy-based mechanisms (MTA-STS, DANE) requiring TLS transmission
• Used for messages where delivery is definitely more important than security
• No assurance that header field will be heeded by any particular MTA
REQUIRETLS SMTP option

• Must be negotiated (with STARTTLS) to send a message tagged as requiring TLS
  – Presence of option represents a promise to require TLS downstream

• Options:
  – Require DNSSEC MX lookup
  – Restrict certificate verification (DANE, cert chain)
  – NO option has been removed
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!
BACKUP SLIDES
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?