Cleartext Considered Obsolete: Best Current Practices for Use of TLS for Email Submission and Access

Keith Moore / Chris Newman
IETF 99
Changes since -06

• Document rewritten to be a BCP
  – -06 was a mixture of protocol and best practice; -07 removes protocol bits that would need to be subject to interoperability tests required of standards track.
  – Some rearrangement of text, significant reduction in size
  – STS stuff removed because it’s all protocol
  – More SHOULDs, fewer MUSTs
Not changed

- Goal is the same: email traffic between UA and MSP should be encrypted
- IMPLICIT TLS preferred over STARTTLS
- Port 465 still recommended for SMTP Submission over TLS (despite conflicting use)
BCPs for MSPs

- Provide IMPLICIT TLS versions of supported services
- Also provide STARTTLS versions in the near term
- Advertise services using DNS SRV records (RFC 6186)
  - Should be signed using DNSSEC
  - Prefer TLS services to non-TLS in advertisements
- Advertise TLSA records (but only if signed by DNSSEC)
- “Deprecate” cleartext mail services “as soon as practicable”
- Transition users to TLS 1.1 or later as soon as practicable
  - Exceptions can be made for legacy MUAs
  - How the transition is accomplished is an MSP decision
BCPs for MUAs

• Support RFC 6186 (SRV records) for discovery of services during account configuration
  – Except: prefer TLS to non-TLS

• Be configurable to require minimum level of confidentiality on a per-account basis
  – TLS 1.1 or later + valid certificate
  – Don’t exchange information if minimum level of confidentiality not met

• For accounts configured without minimum level of confidentiality requirement, opportunistically use TLS when available

• Offer to upgrade cleartext accounts to require minimum confidentiality when TLS becomes available