Email and TLS

draft-ietf-uta-email-deep-01

Keith Moore & Chris Newman

IETF 93 UTA WG

DEEP Overview

- Focus on MUAs IMAP/POP/Submission (does not cover MTA relay)
- Confidentiality Assurance Level for mail account (UI indicator, TLS use, cert verification)
- Prefer Implicit TLS over STARTTLS
- Security Tags, Latching (like HSTS)
- Logging/reporting, Protocol Details

Changes in draft (a)

- Update and clarify abstract
- Use term confidentiality instead of privacy in most cases.
- Move certificate pinning sub-section to account setup section and attempt to define it more precisely.
- Add note about end-to-end encryption in AVAS section.

Changes in draft (b)

- Swap order of DNSSEC and TLSA sub-sections.
- Change meaning of 'tls10' and 'tls12' latches to require certificate validation.
- Replace cipher suite advice with reference to RFC 7525. Change examples to use TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as cipher.

Changes in draft (c)

- Add text to update IMAP, POP3 and Message Submission standards with newer TLS advice.
- Add clearer text in introduction that this does not cover SMTP relay.
- Update references to uta-tls-certs.
- Recommend STARTTLS for SMTP Submission in addition to Implicit TLS.

Open Issues

- Need to update more text related to tls10 & tls12 latches requiring cert validation.
- Email version of RFC 7469 (public key pinning)? Anyone able to propose text?
- Deployment data on port 465 vs. 587 would be helpful. I don't have cycles to gather this data.