Email and TLS

draft-newman-email-deep

Keith Moore & Chris Newman

One Slide Overview

- Focus on MUAs IMAP/POP/Submission
- Prefer Implicit TLS over STARTTLS
- Require TLS for new accounts
- Log cipher suite used
- Security Tags and Latching
- Implementation Requirements

Planned Changes

- Add “imaps”, “pops” URL scheme
- Extensibility for DEEP status
- Better discussion of TLSA/DANE records, including interaction with SRV records
- SNI reference (RFC 6066)
- Finish IANA considerations, more examples.

Controversial Issue (port 465)

- Register "submissions" service (RFC 6409 + TLS) on port 465. Submissions widely deployed already, but port registered for a different use.
- Creates "wart" in registry, so need to build rough consensus beyond WG early.

Open Issue – DNS-ID/ SRV-ID support

- Do we have interoperability testing data for TLS stacks in email clients and servers?
- SRV-ID deployment experience in other protocols?
- RFC 6186 (SRV for email) deployment?

DANE for Submission

- Should we fully define DANE for SMTP Submission? Should we prefer DANE?
- Similar to DANE for SMTP relay but with SRV (RFC 6186) instead of MX. Cert validation works if Submission server explicitly configured but solution for SRV records probably not deployed.

Open Issue – Cipher Suites

- Currently documents already-defined cipher requirements from IMAP & TLS 1.2.
- Q: Add new cipher requirements or defer for common UTA work?

Open Issue – provisional vs. normal

- Is per-server "provisional vs. normal" status sufficient, or more granularity needed?
- Would more granularity be implemented correctly?

Open Issue – PFS latch

- What happens if cipher suite with PFS is found to be flawed and must be disabled, resulting in failure of PFS latch?

Open Issue (sec 8.3)

- Current draft has authenticated-TLS bias; requires it in as many cases as possible even if intrusive to user.
- Will users/admins avoid authenticated TLS if too difficult?
- Should we make unauthenticated TLS easier as alternative to in-the-clear?

Open Issues - Split Document

- Should security tags and latching be split from document?
- Pro: new idea, may delay publication
- Con: latching improves ability to upgrade from unauthenticated encryption, encourages PFS deployment and use
- Suggestion: Too early to decide

Other Open Issues