Email and TLS

draft-ietf-uta-email-deep-01

Keith Moore & Chris Newman

IETF 95 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 -01

- Change tls10 security tag to tls11
- Clarify certificate rules
- Remove old open issues section
- typos in example, etc.

Changes in -02

- Update DANE SMTP reference
- Wording, references improvements

Changes in -03

- Add more references to uta-tls-certs draft; move 6125 to informative

Changes targeting -04

- Reorganize and rework text to make advertise + validate + latch algorithm clearer.
- Add text about versioning security tags for tls11 and tls12
- Change tls-cert reference to new RFC
- Update DANE reference as suggested

Open Issues

- Rename proposal from “DEEP” to “MUA STS” (SMTP STS alignment)
- Change delimiter between security tags from SP to “,” to be more URI friendly (SMTP STS alignment)
- Allow transition between tls-cert and tls-dane-tlsa with option to latch both?

SMTP STS alignment

- Would like SMTP STS to just reference DEEP security tag registry and add tags it needs (to avoid SMTP STS having to design own redundant registry for extensibility). Is DEEP registry model missing anything else that's needed?
- array-of-tags vs key=value?

Possible options to improve SMTP STS

Chris Newman

IETF 95 UTA WG

Context

- I would like the best possible SMTP STS proposal to move forward.
- Brainstorming to make proposal better.
- Believe debate will improve SMTP STS understanding even if my ideas are or are not selected by WG.

SMTP Network Cost

- Mail relay today: DNS lookup + SMTP connection
- With DANE: 2 DNS lookup + SMTP connection
- With DANE+STS: 3 DNS lookups + HTTP connection + SMTP connection
  - Can we avoid 3rd DNS lookup?

Submission vs. Relay I

- DEEP uses deployed cert validation for in-protocol SMTP submission policy.
- Can SMTP STS use in-protocol model?
  - unique-to-relay problems: untrusted MX, multi-domain hosting without early indicator, multi-site MX hosts.

Submission vs. Relay 2

- Untrusted MX: use DNSSEC or PKIX to fixed path server to trust MX or ignore in-protocol policy
- multi-domain hosting: Could use ALPN- (RFC 7301) like mechanism to inform SMTP relay of target domain without a new round-trip (or add 1 round-trip)
- Multi-site MX hosts: not often needed, propose ignoring

Self-Hosting Domain

- For a self-hosting mail domain, we should be able to get MX trust as long as all MX records are in that mail domain and have valid PKIX for that domain.
    - Maybe a key usage PKIX attribute?
- This would save an HTTPS operation for that domain
- A special case, but an important one for large sites.

SMTP Attack Surface

- Attack surface for core SMTP relay is SMTP + TLS + DNS protocols (plus any 822/MIME parsing done by MTA/MDA)
- SMTP STS adds full HTTP client to attack surface. Not sure that's a good idea.
  - Could profile HTTP client (no 2.0, proxy, chunking, keep alive required)
  - Maybe SMTP-521 redirect server?