TLS Attacks & Best Practices

Yaron Sheffer, Ralph Holz & Peter Saint-Andre

UTA WG

IETF 89, London

TLS Attacks

- Moved to separate document:

  draft-sheffer-uta-tls-attacks

- Are we missing any major attacks?

- Should we reference additional publications in the literature?

Best Practices

- draft-sheffer-tls-bcp refactored to focus on our recommendations for software developers and service operators

- Coverage: TLS versions, fallback to SSL, cipher suites, public key length, compression, session resumption

- Are the recommendations sane?

- Are we missing coverage on any important topics?

XMPP / Template

- draft-saintandre-xmpp-tls refactored to mostly reference draft-sheffer-tls-bcp

- Still some text about XMPP-specific issues (SNI equivalent, unauthenticated connections with Server Dialback, human factors / UI guidelines)

- Does this point toward a “template” for other application protocols?