DPRIVE TLS/DTLS Profile and Message Flows

draft-wing-dprive-profile-and-msg-flows-00

November 2015

IETF 94

Authors: T. Reddy, D. Wing and P. Patil

Presenter : Dan Wing

Scope of Document

- TLS and DTLS profiles (normative)
- TLS and DTLS message flows (informative)

(D)TLS profile for DNS privacy

- TLS session resumption without server-side state [RFC5077]
- TLS False Start [draft-ietf-tls-falsestart]
- Cached Information Extension [draft-ietf-tls-cached-info]
- Raw public keys [RFC7250]
- Recommendations for Secure TLS/DTLS [RFC7525]
- DTLS Heartbeat (for just DTLS?)

Message Flows

- Rare events show round trip time advantage for DTLS
  - Server state loss (also occurs with anycast)
  - NAT/firewall state loss

Next steps

- Move (D)TLS profile new draft
  - Probably consolidate with DNSoDTLS's server authentication text?
- Make Message Flows informational
- Adoption of the draft

Questions ?