MUD (D)TLS profiles for IoT devices

draft-ietf-opsawg-mud-tls-06

July 2022

T. Reddy (Nokia)
D.Wing (Citrix)
B.Anderson (Cisco)

Agenda

- Updates to drafts
- Questions & Comments

Updates to draft

- The middlebox must follow the behavior discussed in TLS 1.3 spec to act as a compliant proxy.
- It is **strongly RECOMMENDED** to not act as a TLS proxy wherever possible
  - Bypass TLS proxy functionality or payload inspection for connections destined to specific well-known services.
  - IoT device could be configured to reject all sessions that involve proxy servers to specific well-known services.

Updates to draft

- Network-designated encrypted resolver (DoH/DoT) required to allow MUD policy enforcement.

Updates to draft (Encrypted Client Hello)

- The middlebox would have to follow the behavior in draft-ietf-tls-esni to disable ECH.
  - It can fake ECH records in the DNS response so that the ClientHelloInner can be decrypted by it.
  - It can strip the ECH record from the DNS response.
    - If the client performs full DNSSEC validation locally, it can detect forged DNS responses.

draft-ietf-opsawg-mud-tls-06

- Comments and suggestions are welcome
- Ready for WGLC