TLS/DTLS 1.3 Profiles for the Internet of Things

draft-ietf-uta-tls13-iot-profile-05

Updates

0-RTT signalling for CoAP

- To use 0-RTT, CoAP needs an application profile
- Until -04 we defined the needed signalling extensions (Early-Data Option and Too Early status code) modelled on RFC8740
- CoRE WG did not show interest to use 0-RTT (at least for now)
- Parked the feature in a separate I-D and replaced the section contents with a "MUST NOT use 0-RTT in CoAP"

Fault Attacks on Deterministic Signature Schemes

- TLS 1.3 "[...] RECOMMENDED that implementations implement "deterministic ECDSA" as specified in [RFC6979]"
- Fault attacks such as Poddebniak17 are challenging the existing recommendation
- Most of these attacks assume physical access to the device
  - Especially relevant to smart cards and IoT deployments with poor or non-existent physical security

Fault Attacks on Deterministic Signature Schemes (cont.)

- Private key extraction in a safety-critical system is not fun
- Good CSPRNG in constrained / low-end devices is also quite challenging
- Added a recommendation to combine both randomness and determinism, e.g. using draft-mattsson-cfrg-det-sigs-with-noise if the threat model includes physical / proximity attacks

Editorial

MCR's review excerpt:

> A long thread at LAMPS two years suggests that the term "Intermediate CA" applies only to cross-certification authoritiy bridges, and the term "Subordinate CA" should be used. That this is consistent with history going back to RFC4949.

=> s/Intermediate CA/Subordinate CA/g

Up Next

1.2 -> 1.3 Feature Disparity Fallout

For example:

- Without renego, we need to come up with sensible recommendations for semi-permanent, mutually authenticated connections that need to rekey and check the associated certificate credentials
  - This is a common use case in industrial IoT

See #8

Waiting on MCR's input

- Client cert validation
- Hiding SNI

See #22 and #21

Timers profiling

- For retransmission during handshake
- For RRC during path probing

See #13 and #18