Datagram Transport Layer Security (DTLS) 1.2 Profile for the Internet of Things

draft-ietf-dice-profile-03.txt

Hannes Tschofenig

Status

- Presentation at London IETF meeting identified a number of open issues
  - https://tools.ietf.org/wg/dice/trac/query?component=profile
- New document version addresses open issues:
  - http://tools.ietf.org/html/draft-ietf-dice-profile-03

Closed Issues: Summary

- #1 TLS Compression
- #2 Keep-Alive Extension
- #3 Perfect Forward Secrecy
- #4 Random Number Generation
- #5 Client Certificate URLs
- #6 Trusted CA Indication
- #7 Truncated MAC extension
- #8 Server Name Indication
- #9 Maximum Fragment Length Negotiation

Open Issue

- #10 Depth of Certificate Chain

Section 7 of describes the use of certificate with DTLS. In this context a question arises whether **recommendations regarding the depth of the certificate chain** should be made? Is it useful to indicate an limit in this document or is this too deployment specific? What has been used in other organizations and in deployments?

Document Scope

- Currently, document focuses on the IoT device interacting with cloud-based infrastructure.
  - Client is constrained – server isn't.
- Suggestion was made to also cover the case where client and server are constrained.
  - Example: local peer-to-peer interaction.
- Recommendation:
  - Keep document focused on one design pattern
  - Peer-to-peer case depends on ACE work.

Topics for Investigation

- Support for draft-ietf-tls-encrypt-then-mac-02
  - Means of switching to the more secure encrypt-then-MAC construction as part of the TLS/DTLS handshake, replacing the current MAC-then- encrypt construction.
- Support for draft-bhargavan-tls-session-hash-00
  - TLS master secret is not cryptographically bound to important session parameters such as the client and server identities.
- Support or removal of DTLS Renegotiation
  - Rekeying, client authentication
- Support for Named groups
  - draft-gillmor-tls-negotiated-dl-dhe-02
- Remove GMT time from the ClientHello.
  - draft-mathewson-no-gmtunixtime-00

Next Steps

- Looking for a reviewer.
  Ideal skill set:
  - Familiar with TLS specifications
  - Implementation know-how
  - Deploys DTLS/TLS in an embedded environment
- WGLC end of August / Early September