Practical Issues with DTLS

draft-hartke-dice-practical-issues

IETF 88

Klaus Hartke

DICE Charter

"The third task of the working group is to investigate practical issues around the DTLS handshake in constrained environments.

Many current systems end up fragmenting messages, and the re-transmission and re-ordering of handshake messages results in significant complexity and reliability problems.

Additional reliability mechanisms for transporting DTLS handshake messages are required as they will ensure that handling of re-ordered messages needs to be done only once in a single place in the stack.

The DICE working group may also look at alternative TLS transports in cooperation with the TLS WG."

Step 0. DTLS is the right choice for Constrained Environments –
but we have the feeling that there is room for improvement

Step 1. Document practical issues with DTLS in Constrained Environments 3 4 5

Step 2. Solve the issues:

Implementation Guidance	Profile: Cipher Suites and Extensions	Improvements in TLS	New, optimized transport for TLS
1 2	4	TLS 1.3 wish list 8 9	
LWIG	***DICE***	***TLS***	***DICE***

Step 3. Define the scope of the work
Document the requirements
Establish criteria for the evaluation of possible solutions

Step 4. Propose solutions 3 6 7

Step 5. Evaluate the proposed solutions
Adopt a solution as working group document

1. Kumar, S., Keoh, S., and H. Tschofenig, “A Hitchhiker's Guide to the (Datagram) Transport Layer Security Protocol for Smart Objects and Constrained Node Networks”, draft-ietf-lwig-tls-minimal-00 (work in progress), September 2013.
2. Keoh, S., Kumar, S., and O. Garcia-Morchon, “Securing the IP-based Internet of Things with DTLS”, draft-keoh-lwig-dtls-iot-02 (work in progress), August 2013.
3. Hartke, K., “Practical Issues with Datagram Transport Layer Security in Constrained Environments”, draft-hartke-dice-practical-issues-00 (work in progress), October 2013.
4. Keoh, S., Kumar, S., and Z. Shelby, “Profiling of DTLS for CoAP-based IoT Applications”, draft-keoh-dtls-profile-iot-00 (work in progress), June 2013.
5. Sethi, M., Arkko, J., Keranen, A., and H. Rissanen, “Practical Considerations and Implementation Experiences in Securing Smart Object Networks”, draft-aks-crypto-sensors-02 (work in progress), March 2012.
6. Bormann, C., “6LoWPAN Generic Compression of Headers and Header-like Payloads”, draft-bormann-6lo-ghc-00 (work in progress), October 2013.
7. Raza, S., Trabalza, D., and T. Voigt, “Lithe: Lightweight Secure CoAP for the Internet of Things”, IEEE Sensors Journal, Volume 13, Issue 10, August 2013.
8. Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Out-of-Band Public Key Validation for Transport Layer Security (TLS)", draft-ietf-tls-oob-pubkey-09 (work in progress), July 2013.
9. Santesson, S. and H. Tschofenig, "Transport Layer Security (TLS) Cached Information Extension", draft-ietf-tls-cached-info-14 (work in progress), March 2013.