DICE Working Group
Internet-Draft
Intended status: Informational
Expires: June 22, 2014

K. Hartke, Ed.
Universitaet Bremen TZI

December 19, 2013

A DTLS Profile for the Internet of Things
draft-hartke-dice-profile-02

Abstract

This document defines a DTLS profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.

Disclaimer

This is a very early, very rough draft. At this stage, the draft is not intended to make any specific proposal for a profile, but aims to create a shared understanding of what a DTLS profile defines. No security analysis has been performed.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 22, 2014.

Copyright Notice

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document defines a DTLS 1.2 [RFC6347] profile that enables secure and private exchange of information in Internet of Things applications and is reasonably implementable on many constrained devices.

- One-stop list of RFCs to be implemented.
- No changes to TLS or DTLS.
- No new extensions defined by the profile.
- No negotiation of the profile between client and server.
- Profile avoids doing things the TLS WG decided not to do.
- Profile aligns with the DTLS security modes of the Constrained Application Protocol (CoAP) [I-D.ietf-core-coap].

- Profile takes advantage of existing hardware support where possible.
- Document includes a brief discussion of extensions not included.

2. Profile

2.1. Applicability

- Communication Model
- Threat Model
- Security Requirements
- Classes of Devices [I-D.ietf-lwig-terminology]
- Trust Model
- ...

2.2. Cipher Suites

- Specific Cipher Suite(s) -vs- Cryptographic Agility
- Server Authentication -vs- Mutual Authentication
- X.509 Certificates -vs- Raw Public Keys -vs- Pre-Shared Keys
- Perfect Forward Secrecy
- Only AEAD Cipher Suites
- ...

2.3. Extensions

- Signature Algorithms [RFC5246]
- Server Name Indication [RFC6066]

- Maximum Fragment Length [RFC6066]
- Client Certificate URLs [RFC6066]
- Truncated HMAC [RFC6066]
- Certificate Status Request [RFC6066]
- Supported Elliptic Curves [RFC4492]
- Supported Point Formats [RFC4492]

- Application Layer Protocol [I-D.ietf-tls-applayerprotoneg]
- Cached Info [I-D.ietf-tls-cached-info]
- Session Resumption without Server-Side State [RFC5077]
- Renegotiation Indication [RFC5746]
- Heartbeat [RFC6520]
- ...

2.4. Other

- Timer Values
- Compression
- Renegotiation -vs- Reconnection
- Session Resumption (with Server-Side State)
- Extended Session Resumption [I-D.hummen-dtls-extended-session-resumption]
- Replay Protection
- Certificate Revocation

- Encrypt-then-MAC [I-D.gutmann-tls-encrypt-then-mac]
- Hash Algorithm [I-D.campagna-suitee]
- ...

3. Implementation Considerations

- [I-D.sheffer-tls-bcp]
- [I-D.ietf-lwig-tls-minimal]
- [I-D.ietf-lwig-guidance]
- Random Number Generation [RFC4086]
- Denial-of-Service Countermeasures [RFC6347]
- Cipher Suite Negotiation

- Version Negotiation [I-D.pettersen-tls-version-rollback-removal] [I-D.bmoeller-tls-downgrade-scsv]
- Upgrade from Server-Authenticated to Mutually-Authenticated
- Common Implementation Pitfalls
- ...

4. Privacy Considerations

- [RFC6973]
- [I-D.cooper-ietf-privacy-requirements]
- Meta Data
- Traffic Patterns
- Fingerprinting
- ...

5. Security Considerations

- [RFC3552]
- ...

6. IANA Considerations

This document includes no request to IANA.

7. Acknowledgements

Thanks to Rene Hummen, Sye Loong Keoh, Sandeep Kumar, Eric Rescorla, Zach Shelby, Hannes Tschofenig, and Sean Turner for helpful comments and discussions that have shaped the document.

8. References

8.1. Normative References

[I-D.ietf-tls-applayerprotoneg]
Friedl, S., Popov, A., Langley, A., and S. Emile, "Transport Layer Security (TLS) Application Layer Protocol Negotiation Extension", draft-ietf-tls-applayerprotoneg-03 (work in progress), October 2013.

[I-D.ietf-tls-cached-info]
Santesson, S. and H. Tschofenig, "Transport Layer Security (TLS) Cached Information Extension", draft-ietf-tls-cached-info-15 (work in progress), October 2013.

[I-D.ietf-tls-oob-pubkey]
Wouters, P., Tschofenig, H., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", draft-ietf-tls-oob-pubkey-10 (work in progress), October 2013.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5746] Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, February 2010.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6520] Seggelmann, R., Tuexen, M., and M. Williams, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension", RFC 6520, February 2012.

8.2. Informative References

[I-D.bmoeller-tls-downgrade-scsv]
Moeller, B., "TLS Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks", draft-bmoeller-tls-downgrade-scsv-00 (work in progress), September 2013.

[I-D.campagna-suitee]
Campagna, M., "A Cryptographic Suite for Embedded Systems (SuiteE)", draft-campagna-suitee-04 (work in progress), October 2012.

[I-D.cooper-ietf-privacy-requirements]
Cooper, A., Farrell, S., and S. Turner, "Privacy Requirements for IETF Protocols", draft-cooper-ietf-privacy-requirements-01 (work in progress), October 2013.

[I-D.greevenbosch-tls-ocsp-lite]
Greevenbosch, B., "OCSP-lite - Revocation of raw public keys", draft-greevenbosch-tls-ocsp-lite-01 (work in

progress), June 2013.

[I-D.gutmann-tls-encrypt-then-mac]
Gutmann, P., "Encrypt-then-MAC for TLS and DTLS", draft-gutmann-tls-encrypt-then-mac-04 (work in progress), October 2013.

[I-D.hummen-dtls-extended-session-resumption]
Hummen, R., Gilger, J., and H. Shafagh, "Extended DTLS Session Resumption for Constrained Network Environments", draft-hummen-dtls-extended-session-resumption-01 (work in progress), October 2013.

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., and C. Bormann, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18 (work in progress), June 2013.

[I-D.ietf-lwig-guidance]
Bormann, C., "Guidance for Light-Weight Implementations of the Internet Protocol Suite", draft-ietf-lwig-guidance-03 (work in progress), February 2013.

[I-D.ietf-lwig-terminology]
Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained Node Networks", draft-ietf-lwig-terminology-05 (work in progress), July 2013.

[I-D.ietf-lwig-tls-minimal]
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.

[I-D.pettersen-tls-version-rollback-removal]
Pettersen, Y., "Managing and removing automatic version rollback in TLS Clients", draft-pettersen-tls-version-rollback-removal-02 (work in progress), August 2013.

[I-D.sheffer-tls-bcp]

Sheffer, Y. and R. Holz, "Recommendations for Secure Use of TLS and DTLS", draft-sheffer-tls-bcp-01 (work in progress), September 2013.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

Author's Address

Klaus Hartke (editor)
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63905
Email: hartke@tzi.org