DICE Working Group
Internet-Draft
Intended status: Informational
Expires: May 08, 2014

K. Hartke
Nokia

November 04, 2013

A DTLS Profile for the Internet of Things
draft-hartke-dice-profile-00

Abstract

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

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 May 08, 2014.

Copyright Notice

Internet-Draft A DTLS Profile for the Internet of Things November 2013

Table of Contents

1. Introduction

This document defines a DTLS 1.2 [RFC6347] profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.

...

2. Profile

2.1. Applicability

- Communication Model
- Threat Model
- Security Requirements
- Classes of Devices
- 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
- ...

2.3. Extensions

- Signature Algorithms [RFC5246]
- Server Name Indication [RFC6066]
- Maximum Fragment Length [RFC6066]
- Certificate Status Request [RFC6066]
- Truncated HMAC [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]
- Snap Start [I-D.agl-tls-snapstart]
- Renegotiation Indication [RFC5746]
- Heartbeat [RFC6520]
- ...

2.4. Other

- Compression
- Renegotiation -vs- Reconnection
- Session Resumption
- Replay Protection
- Timer Values

- Certificate Revocation
- Encrypt-then-MAC [I-D.gutmann-tls-encrypt-then-mac]
- Hash Algorithm
- ...

3. Implementation Considerations

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

4. Privacy Considerations

- ...

5. Security Considerations

- ...

6. IANA Considerations

o ...

7. Acknowledgements

Thanks to Hannes Tschofenig, Sye Loong Keoh, and Rene Hummen 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.

[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.agl-tls-snapstart]
Langley, A., "Transport Layer Security (TLS) Snap Start", draft-agl-tls-snapstart-00 (work in progress), June 2010.

[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.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-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.

Author's Address

Klaus Hartke
Nokia
Hermiankatu 12 D
Tampere FI-33720
Finland

Email: klaus.hartke@nokia.com