Abstract

This document describes using a session layer service for DOTS messaging to provide secure messaging while delivering on a number of DOTS requirements including avoiding fate-sharing with the underlying communications.

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 September 22, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents 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.
1. Introduction

The DOTS requirements [I-D.ietf-dots-requirements] includes

- Reduced fate-sharing
- Perform well during times of high congestion

These requirements are at best challenging to meet with the traditional IETF communication building blocks of TCP+TLS or UDP+DTLS. Recent work [I-D.hares-i2nsf-ssls] present a new/old way of isolating the DOTS protocol from the fate of the Internet Transport protocols by providing an OSI-styled Session Layer that provides:

- Data chunking
- Data compression
- Fully peered data security
- Survivability of security state

A session layer approach to DOTS would allow a single DOTS client/server communication to be selective on transport technology to the appropriate one for a given situation. For example without requiring additional security management, a TCP connection can be used for large transfers during un-congested times. Communications can switch to UDP during congestion caused by an on-going attack. Even SMS (if
directly supported by the DOTS agents) can be employed to get the message out during an attack. All this with a single, manageable state between the DOTS client and agent.

The intelligence to make the transport decision and the knowledge as to parameters like appropriate chunking size is managed in the session layer.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.2. Definitions

DSRC: (Dedicated Short Range Communications) is a two-way short- to-medium-range wireless communications capability that permits very high data transmission critical in communications-based automotive active safety applications.

3. Problem Space

The communication problems faced by DOTS are defined in the DOTS requirements [I-D.ietf-dots-requirements]. General requirements 2, 3 and 4: Resilience and Robustness, Bidirectionality, and Sub-MTU Message size, present challenges to current IETF communication tools. Only IPsec approaches a good fit to these requirements.

3.1. The cryptographic state conundrum

The cost for cryptography can come through frequent asymmetric key operations as in DKIM [RFC5585] and DSRC’s IEEE 1609.2 [IEEE.1609.2-2013] or maintaining communications security state as in TLS, DTLS, and IPsec.

DKIM can afford asymmetric key operations as it works on a loose timing basis. DSRC is requiring dedicated asymmetric key hardware in each car; the consumer will be absorbing those costs. DOTS does not have the sub-second timing requirements like DSRC, nor does it have the minutes leeway of DKIM. It is unlikely that the many DOTS clients will have the processing power for asymmetric key operations during a DDoS attack. Thus DOTS should rely on one of the stateful secure communications technologies.
Stateful secure communications implies some method of maintaining this state, especially during an active attack. Both TLS and DTLS share fate with the underlying transport. This means that if either the DOTS client or server is forced to reboot due to an attack (or any other reason), the D/TLS state needs to be reset. For a DOTS client under attack, this can be a processor expensive operation and may fail out of hand if the downlink is flooded with attack traffic and the server response is lost. The DOTS server has the additional conundrum as how to notify the client to reset the lost security state in a manner that does not introduce yet another attack.

### 3.1.1. IPsec not a solution

IKEv2 [RFC7296] can be started from either participant. This means that a DOTS server can reset the security state as part of its reboot process. ESP [RFC4303] in transport mode provides a familiar approach to protect UDP traffic. ESP with IKEv2 fate-shares with both IP and UDP. The loss of UDP state due to a DOTS server crash would require reestablishment of the security state. This keeps attacks against the DOTS server as an important attack surface to weigh against the familiarity of ESP with IKEv2.

ESP limits secure DOTS messaging to IP networks. A different method would be needed for sending DOTS messages over SMS or require IP over a modem connection.

ESP NAT traversal uses UDP and thus reintroduces the UDP blocking concern discussed above.

### 4. Introducing a Session Layer Service

The DOTS communication and security requirements can solved by moving above the transport and define an OSI-styled session layer. A session-layer service would not fate-share with the underlying transport. A peer-based KMP like IKEv2 or HIPv2 [RFC7401] can be initiated by either side, making recovery of security state straightforward. Further, if the security state is maintained in a secure store that can survive a system reboot, no resetting of the security state would be necessary after a reboot. This would make an attack that causes a DOTS agent to reboot less interesting.

#### 4.1. Services provided at Session Layer

Six key services are built into [I-D.hares-i2nsf-ssl]:

- KMP negotiation of compression and security
- Data chunking
5. IANA Considerations

No IANA considerations exist for this document at this time.

6. Security Considerations

A session layer security approach leaves the lower layers open to attack. These attacks should not impact the DOTS application or session security. At most they form yet another DoS attack against the DOTS agents. This cost is considered acceptable balanced by the gains against other attacks if the security and other related services are moved back down the stack.

7. Contributors

TBD

8. References

8.1. Normative References


8.2. Informative References

[I-D.hares-i2nsf-ssls]

[I-D.ietf-dots-requirements]
[I-D.moskowitz-sse]
Moskowitz, R., Faynberg, I., Lu, H., Hares, S., and P.
Giacomin, "Session Security Envelope", draft-moskowitz-
sse-03 (work in progress), March 2016.

[IEEE.1609.2-2013]
"IEEE Standard for Wireless Access in Vehicular
Environments--Security Services for Applications and

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",
RFC 4303, DOI 10.17487/RFC4303, December 2005,

Identified Mail (DKIM) Service Overview", RFC 5585,
DOI 10.17487/RFC5585, July 2009,

Kivinen, "Internet Key Exchange Protocol Version 2
(IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October

Henderson, "Host Identity Protocol Version 2 (HIPv2)",
RFC 7401, DOI 10.17487/RFC7401, April 2015,

Authors’ Addresses

Robert Moskowitz
HTT Consulting
Oak Park, MI  48237

Email: rgm@labs.htt-consult.com

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI  48176
USA

Email: shares@ndzh.com