Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 17, 2013

R. Jesup
WorldGate Communications
S. Loreto
Ericsson
R. Stewart
Adara Networks
M. Tuexen
Muenster Univ. of Appl. Sciences
July 16, 2012

DTLS Encapsulation of SCTP Packets for RTCWEB
draft-tuexen-tsvwg-sctp-dtls-encaps-01.txt

Abstract

The Stream Control Transmission Protocol (SCTP) is a transport protocol originally defined to run on top of the network protocols IPv4 or IPv6. This memo document specifies how SCTP can be used on top of the Datagram Transport Layer Security (DTLS) protocol. SCTP over DTLS is used by the RTCWeb protocol suite for transporting non-media data between browsers.

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 January 17, 2013.

Table of Contents

1. Introduction

1.1. Overview

The Stream Control Transmission Protocol (SCTP) as defined in [RFC4960] is a transport protocol running on top of the network protocols IPv4 or IPv6. This memo document specifies how SCTP can be used on top of the Datagram Transport Layer Security (DTLS) protocol. SCTP over DTLS is used by the RTCWeb protocol suite (see [I-D.ietf-rtcweb-overview] for an overview) for transporting non-media data between browsers. The architecture of this stack is described in [I-D.jesup-rtcweb-data].

1.2. Terminology

This document uses the following terms:

Association: An SCTP association.

Stream: A unidirectional stream of an SCTP association. It is uniquely identified by a stream identifier.

1.3. Abbreviations

DTLS: Datagram Transport Layer Security.

MTU: Maximum Transmission Unit.

PPID: Payload Protocol Identifier.

SCTP: Stream Control Transmission Protocol.

TCP: Transmission Control Protocol.

TLS: Transport Layer Security.

2. Conventions

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 [RFC2119].

3. Encapsulation and Decapsulation Procedure

When an SCTP packet is sent down to the DTLS layer, the complete SCTP packet, consisting of the SCTP common header and a number of SCTP

chunks, MUST be handled as the payload of the application layer protocol of DTLS. When the DTLS layer has processed a DTLS record containing a message of the application layer protocol, the payload MUST be given up to the SCTP layer. The SCTP layer expects an SCTP common header followed by a number of SCTP chunks.

4. DTLS Considerations

The DTLS implementation MUST be based on [RFC6347].

If path MTU discovery is performed by the DTLS layer, the method described in [RFC4821] MUST be used. For probe packets, the extension defined in [RFC6520] MUST be used.

If path MTU discovery is performed by the SCTP layer and IPv4 is used as the network layer protocol, the DTLS implementation MUST allow the DTLS user to enforce that the corresponding IPv4 packet is sent with the DF bit set.

SCTP performs segmentation and reassembly based on the path MTU. Therefore the DTLS layer MUST NOT use any compression algorithm.

5. SCTP Considerations

5.1. Base Protocol

SCTP as specified in [RFC4960] is used. However, the following restrictions are necessary to reflect that the lower layer is the connection oriented protocol DTLS instead of the connection less protocol IPv4 and IPv6:

- A DTLS connection MUST be established before an SCTP association can be set up.
- All associations MUST be single-homed.
- The INIT and INIT-ACK chunk MUST NOT contain any IPv4 Address or IPv6 Address parameters. The INIT chunk MUST NOT contain the Supported Address Types parameter.
- The implementation MUST NOT rely on processing ICMP or ICMPv6 packets. This applies in particular to path MTU discovery when performed by SCTP.
- The DTLS implementation might not allow the setting of ECN bits for outgoing packets or provide the ECN bits for incoming packets.

In this case, SCTP MUST NOT use ECN.

- The DTLS implementation might not allow the setting of DF bit for outgoing packets. In this case, SCTP can't perform path MTU discovery.

5.2. Padding Extension

The padding extension defined in [RFC4820] MUST be supported and used for probe packets when performing path MTU discovery as specified in [RFC4821].

5.3. Dynamic Address Reconfiguration Extension

The SCTP implementation MUST support the Supported Extensions Parameter defined in [RFC5061] to signal the support of the SCTP stream reset extension (see Section 5.6). The other functionality described in [RFC5061] MUST NOT be used.

5.4. SCTP Authentication Extension

The SCTP authentication extension defined in [RFC4895] is not required.

5.5. Partial Reliability Extension

The SCTP implementation MUST support the extension defined in [RFC3758].

The SCTP implementation SHOULD support the following PR-SCTP policies:

- A user message is abandoned after a user specified lifetime.

- A user message is abandoned if the number of retransmissions exceeds a user specified threshold.

5.6. Stream Reset Extension

The SCTP implementation MUST support the SCTP stream reset extension defined in [RFC6525]. It is used to reset streams and add streams during the lifetime of the SCTP association.

5.7. Large User Message Extension

SCTP as defined in [RFC4960] does not support the multiplexing of large user messages that need to be fragmented and reassembled by the SCTP layer. To overcome this limitation, the SCTP implementation

SHOULD support an extension, which has to be defined.

5.8. Congestion Control

In addition to the TCP-like congestion control specified in [RFC4960], other congestion control algorithms MAY be provided. For example, it might be helpful to use a congestion control which does not increase the queueing delay substantially (see [I-D.ietf-ledbat-congestion] for an example).

6. IANA Considerations

This document requires no actions from IANA.

7. Security Considerations

TBD.

8. Acknowledgments

The authors wish to thank XXX for their invaluable comments.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3758] Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., and P. Conrad, "Stream Control Transmission Protocol (SCTP) Partial Reliability Extension", RFC 3758, May 2004.

[RFC4820] Tuexen, M., Stewart, R., and P. Lei, "Padding Chunk and Parameter for the Stream Control Transmission Protocol (SCTP)", RFC 4820, March 2007.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, March 2007.

[RFC4895] Tuexen, M., Stewart, R., Lei, P., and E. Rescorla, "Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)", RFC 4895, August 2007.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5061] Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, September 2007.

[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.

[RFC6525] Stewart, R., Tuexen, M., and P. Lei, "Stream Control Transmission Protocol (SCTP) Stream Reconfiguration", RFC 6525, February 2012.

9.2. Informative References

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-04 (work in progress), June 2012.

[I-D.jesup-rtcweb-data]
Jesup, R., Loreto, S., and M. Tuexen, "RTCWeb Datagram Connection", draft-jesup-rtcweb-data-01 (work in progress), October 2011.

[I-D.ietf-ledbat-congestion]
Hazel, G., Iyengar, J., Kuehlewind, M., and S. Shalunov, "Low Extra Delay Background Transport (LEDBAT)", draft-ietf-ledbat-congestion-09 (work in progress), October 2011.

Authors' Addresses

Randell Jesup
WorldGate Communications
3800 Horizon Blvd, Suite #103
Trevose, PA 19053-4947
US

Phone: +1-215-354-5166
Email: randell_ietf@jesup.org

Salvatore Loreto
Ericsson
Hirsalantie 11
Jorvas 02420
FI

Email: Salvatore.Loreto@ericsson.com

Randall R. Stewart
Adara Networks
Chapin, SC 29036
US

Email: randall@lakerest.net

Michael Tuexen
Muenster University of Applied Sciences
Stegerwaldstrasse 39
48565 Steinfurt
DE

Email: tuexen@fh-muenster.de