Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets

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 document specifies how SCTP can be used on top of the Datagram Transport Layer Security (DTLS) protocol. Using the encapsulation method described in this document, SCTP is unaware of the protocols being used below DTLS; hence, explicit IP addresses cannot be used in the SCTP control chunks. As a consequence, the SCTP associations carried over DTLS can only be single-homed.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8261.
Copyright Notice

Copyright (c) 2017 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
(https://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.

Table of Contents

1. Overview .................................................. 3
2. Conventions ................................................. 3
3. Encapsulation and Decapsulation Procedure .................. 3
4. General Considerations ..................................... 4
5. DTLS Considerations ....................................... 4
6. SCTP Considerations ....................................... 5
7. IANA Considerations ....................................... 6
8. Security Considerations .................................... 7
9. References .................................................. 7
Acknowledgments ............................................... 10
Authors’ Addresses ............................................ 10
1. Overview

The Stream Control Transmission Protocol (SCTP) as defined in [RFC4960] is a transport protocol running on top of the network protocols IPv4 [RFC0791] or IPv6 [RFC8200]. This document specifies how SCTP is used on top of the Datagram Transport Layer Security (DTLS) protocol. DTLS 1.0 is defined in [RFC4347], and the latest version when this RFC was published, DTLS 1.2, is defined in [RFC6347]. This encapsulation is used, for example, within the WebRTC protocol suite (see [RTC-OVERVIEW] for an overview) for transporting non-SRTP data between browsers. The architecture of this stack is described in [DATA-CHAN].

```
+----------+
|   SCTP   |
+----------+
|   DTLS   |
+----------+
| ICE/UDP  |
+----------+
```

Figure 1: Basic Stack Diagram

This encapsulation of SCTP over DTLS over UDP or ICE/UDP (see [RFC5245]) can provide a NAT traversal solution in addition to confidentiality, source authentication, and integrity-protected transfers. Please note that using ICE does not necessarily imply that a different packet format is used on the wire.

Please note that the procedures defined in [RFC6951] for dealing with the UDP port numbers do not apply here. When using the encapsulation defined in this document, SCTP is unaware about the protocols used below DTLS.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Encapsulation and Decapsulation Procedure

When an SCTP packet is provided to the DTLS layer, the complete SCTP packet, consisting of the SCTP common header and a number of SCTP chunks, is 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 is passed to
the SCTP layer. The SCTP layer expects an SCTP common header
followed by a number of SCTP chunks.

4. General Considerations

An implementation of SCTP over DTLS MUST implement and use a path
maximum transmission unit (MTU) discovery method that functions
without ICMP to provide SCTP/DTLS with an MTU estimate. An
implementation of "Packetization Layer Path MTU Discovery" [RFC4821]
either in SCTP or DTLS is RECOMMENDED.

The path MTU discovery is performed by SCTP when SCTP over DTLS is
used for data channels (see Section 5 of [DATA-CHAN]).

5. DTLS Considerations

The DTLS implementation MUST support DTLS 1.0 [RFC4347] and SHOULD
support the most recently published version of DTLS, which was DTLS
1.2 [RFC6347] when this RFC was published. In the absence of a
revision to this document, the latter requirement applies to all
future versions of DTLS when they are published as RFCs. This
document will only be revised if a revision to DTLS or SCTP makes a
revision to the encapsulation necessary.

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

The DTLS MUST support sending messages larger than the current path
MTU. This might result in sending IP-level fragmented messages.

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 SHOULD allow
the DTLS user to enforce that the corresponding IPv4 packet is sent
with the Don’t Fragment (DF) bit set. If controlling the DF bit is
not possible (for example, due to implementation restrictions), a
safe value for the path MTU has to be used by the SCTP stack. It is
RECOMMENDED that the safe value not exceed 1200 bytes. Please note
that [RFC1122] only requires that end hosts be able to reassemble
fragmented IP packets up to 576 bytes in length.

The DTLS implementation SHOULD allow the DTLS user to set the
Differentiated Services Code Point (DSCP) used for IP packets being
sent (see [RFC2474]). This requires the DTLS implementation to pass
the value through and the lower layer to allow setting this value. If the lower layer does not support setting the DSCP, then the DTLS user will end up with the default value used by the protocol stack. Please note that only a single DSCP value can be used for all packets belonging to the same SCTP association.

Using Explicit Congestion Notification (ECN) in SCTP requires the DTLS layer to pass the ECN bits through and its lower layer to expose access to them for sent and received packets (see [RFC3168]). The implementations of DTLS and its lower layer have to provide this support. If this is not possible (for example, due to implementation restrictions), ECN can’t be used by SCTP.

6. SCTP Considerations

This section describes the usage of the base protocol and the applicability of various SCTP extensions.

6.1. Base Protocol

This document uses SCTP [RFC4960] with the following restrictions, which are required to reflect that the lower layer is DTLS instead of IPv4 and IPv6 and that SCTP does not deal with the IP addresses or the transport protocol used below DTLS:

- A DTLS connection MUST be established before an SCTP association can be set up.
- Multiple SCTP associations MAY be multiplexed over a single DTLS connection. The SCTP port numbers are used for multiplexing and demultiplexing the SCTP associations carried over a single DTLS connection.
- All SCTP associations are single-homed, because DTLS does not expose any address management to its upper layer. Therefore, it is RECOMMENDED to set the SCTP parameter path.max.retrans to association.max.retrans.
- 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, since the SCTP layer most likely is unable to access the SCTP common header in the plain text of the packet, which triggered the sending of the ICMP or ICMPv6 packet. This applies in particular to path MTU discovery when performed by SCTP.
o If the SCTP layer is notified about a path change by its lower layers, SCTP SHOULD retest the path MTU and reset the congestion state to the initial state. The window-based congestion control method specified in [RFC4960] resets the congestion window and slow-start threshold to their initial values.

6.2. Padding Extension

When the SCTP layer performs path MTU discovery as specified in [RFC4821], the padding extension defined in [RFC4820] MUST be supported and used for probe packets (HEARTBEAT chunks bundled with PADDING chunks [RFC4820]).

6.3. Dynamic Address Reconfiguration Extension

If the dynamic address reconfiguration extension defined in [RFC5061] is used, ASCONF chunks MUST use wildcard addresses only.

6.4. SCTP Authentication Extension

The SCTP authentication extension defined in [RFC4895] can be used with DTLS encapsulation, but does not provide any additional benefit.

6.5. Partial Reliability Extension

Partial reliability as defined in [RFC3758] can be used in combination with DTLS encapsulation. It is also possible to use additional Partially Reliable Stream Control Transmission Protocol (PR-SCTP) policies, for example, the ones defined in [RFC7496].

6.6. Stream Reset Extension

The SCTP stream reset extension defined in [RFC6525] can be used with DTLS encapsulation. It is used to reset SCTP streams and add SCTP streams during the lifetime of the SCTP association.

6.7. Interleaving of Large User Messages

SCTP as defined in [RFC4960] does not support the interleaving of large user messages that need to be fragmented and reassembled by the SCTP layer. The protocol extension defined in [RFC8260] overcomes this limitation and can be used with DTLS encapsulation.

7. IANA Considerations

This document does not require any IANA actions.
8. Security Considerations

Security considerations for DTLS are specified in [RFC4347] and for SCTP in [RFC4960], [RFC3758], and [RFC6525]. The combination of SCTP and DTLS introduces no new security considerations.

SCTP should not process the IP addresses used for the underlying communication since DTLS provides no guarantees about them.

It should be noted that the inability to process ICMP or ICMPv6 messages does not add any security issue. When SCTP is carried over a connection-less lower layer like IPv4, IPv6, or UDP, processing of these messages is required to protect other nodes not supporting SCTP. Since DTLS provides a connection-oriented lower layer, this kind of protection is not necessary.

9. References

9.1. Normative References


9.2. Informative References

[DATA-CHAN]


Acknowledgments

The authors wish to thank David Black, Benoit Claise, Spencer Dawkins, Francis Dupont, Gorry Fairhurst, Stephen Farrell, Christer Holmberg, Barry Leiba, Eric Rescorla, Tom Taylor, Joe Touch, and Magnus Westerlund for their invaluable comments.

Authors’ Addresses

Michael Tuexen
Muenster University of Applied Sciences
Stegerwaldstrasse 39
48565 Steinfurt
Germany
Email: tuexen@fh-muenster.de

Randall R. Stewart
Netflix, Inc.
Chapin, SC  29036
United States of America
Email: randall@lakerest.net

Randell Jesup
WorldGate Communications
3800 Horizon Blvd, Suite #103
Trevose, PA  19053-4947
United States of America
Phone: +1-215-354-5166
Email: randell-ietf@jesup.org

Salvatore Loreto
Ericsson
Hirsalantie 11
Jorvas  02420
Finland
Email: Salvatore.Loreto@ericsson.com