Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 25, 2009

M. Tuexen
R. Seggelmann
Muenster Univ. of Applied Sciences
E. Rescorla
RTFM, Inc.
October 22, 2008

Datagram Transport Layer Security for Stream Control Transmission Protocol
draft-ietf-tsvwg-dtls-for-sctp-00.txt

Abstract

This document describes the usage of the Datagram Transport Layer Security (DTLS) protocol over the Stream Control Transmission Protocol (SCTP).

The user of DTLS over SCTP can take advantage of all features provided by SCTP and its extensions, especially support of

o multiple streams to avoid head of line blocking.

- multi-homing to provide network level fault tolerance.
- unordered delivery.
- partially reliable data transfer.

Table of Contents

1. Introduction

1.1. Overview

This document describes the usage of the Datagram Transport Layer Security (DTLS) protocol, as defined in [RFC4347], over the Stream Control Transmission Protocol (SCTP), as defined in [RFC4960].

TLS is designed to run on top of a byte-stream oriented transport protocol providing a reliable, in-sequence delivery. Thus, TLS is currently mainly being used on top of the Transmission Control Protocol (TCP), as defined in [RFC0793].

TLS over SCTP as described in [RFC3436] has some serious limitations:

- It does not support the unordered delivery of SCTP user messages.
- It does not support partial reliability as defined in [RFC3758].
- It only supports the usage of the same number of streams in both directions.
- It uses a TLS connection for every bidirectional stream, which requires a substantial amount of resources and message exchanges if a large number of streams is used.

DTLS over SCTP as described in this document overcomes these limitations of TLS over SCTP. The user of DTLS over SCTP can use all services provided by SCTP and its partial reliability extension. The dynamic modification of the IP-addresses used by the SCTP end-points is also supported.

The method described in this document requires that the SCTP implementation supports the optional feature of fragmentation of SCTP user messages and the SCTP authentication extension defined in [RFC4895].

1.2. Terminology

This document uses the following terms:

Association: An SCTP association.

Connection: A TLS connection.

Session: A TLS session.

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

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. DTLS considerations

3.1. Message sizes

DTLS limits the user message size to the current Path MTU. This limit SHOULD be increased to 2^14 Bytes for DTLS/SCTP.

3.2. Message fragmentation

The DTLS layer MUST NOT perform message fragmentation. The SCTP layer will perform this task. Thus the supported maximum length of SCTP user messages MUST be at least 2^14 + 2048 + 5 = 18437 bytes. Every DTLS message MUST be handled as one user message for SCTP.

3.3. Replay detection

Replay detection of DTLS MUST NOT be used.

3.4. Path MTU Discovery

Path MTU discovery of DTLS MUST NOT be used.

3.5. Retransmission of Messages

DTLS procedures for retransmissions MUST NOT be used.

4. SCTP considerations

4.1. Stream usage

All DTLS control messages MUST be transported on stream 0 with unlimited reliability and with the ordered delivery feature.

User data messages MAY be transported over stream 0 but users SHOULD use other streams for better performance.

4.2. Chunk handling

The DATA, SACK and FORWARD-TSN chunks of SCTP MUST be sent in an authenticated way as described in [RFC4895]. Other chunks MAY be sent in an authenticated way.

This makes sure that an attacker can not modify the stream a message is sent in or affect the ordered/unordered delivery of the message. It is also not possible for an attacker to drop messages and use forged FORWARD-TSN and SACK chunks to hide this dropping.

4.3. Handshake

To prevent DTLS from discarding user messages while renegotiating, before sending a ClientHello all user messages MUST have been acknowledged and can not be revoked anymore by the peer.

Prior to sending a HelloVerifyRequest, all user messages MUST be read from the transport layer or user messages MUST be allowed during handshake.

4.4. Handling of endpoint-pair shared secrets

The endpoint-pair shared secret for Shared Key Identifier 0 is empty. Whenever the master key changes, a 64 byte shared secret is derived from every master secret and provided as a new end-point pair shared secret by using the algorithm described in [I-D.ietf-tls-extractor].

The Shared Key Identifier MUST be incremented by 1. If it is 65535, the next value MUST be 1.

Before sending the Finished message the active SCTP-AUTH key MUST be switched to the new one. The Finished message MUST NOT be sent

before all messages except the ones from this handshake have been acknowledged and can not be revoked anymore by the peer.

Once the corresponding Finished message from the peer has been received the old key SHOULD be removed.

5. IANA Considerations

IANA needs to add a value to the TLS Extractor Label registry as described in [I-D.ietf-tls-extractor]. The label suggested is EXTRACTOR_DTLS_OVER_SCTP. The reference should refer to this document.

6. Security Considerations

This section is not complete yet.

7. Acknowledgments

The authors wish to thank Carsten Hohendorf, and Alfred Hoenes for their invaluable comments.

8. References

8.1. 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.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[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.

[I-D.ietf-tls-extractor]

Rescorla, E., "Keying Material Extractors for Transport Layer Security (TLS)", draft-ietf-tls-extractor-02 (work in progress), September 2008.

8.2. Informative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, December 2002.

Authors' Addresses

Michael Tuexen
Muenster Univ. of Applied Sciences
Stegerwaldstr. 39
48565 Steinfurt
Germany

Email: tuexen@fh-muenster.de

Robin Seggelmann
Muenster Univ. of Applied Sciences
Stegerwaldstr. 39
48565 Steinfurt
Germany

Email: seggelmann@fh-muenster.de

Eric Rescorla
RTFM, Inc.
2064 Edgewood Drive
Palo Alto, CA 94303
USA

Email: ekr@networkresonance.com

Full Copyright Statement

Intellectual Property