

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 20, 2008

M. Tuexen
Muenster Univ. of Applied Sciences
E. Rescorla
RTFM, Inc.
November 17, 2007

Datagram Transport Layer Security for Stream Control Transmission
Protocol
draft-tuexen-dtls-for-sctp-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on May 20, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

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

Internet-Draft

DTLS for SCTP

November 2007

- o multiple streams to avoid head of line blocking.
- o multi-homing to provide network level fault tolerance.
- o unordered delivery.
- o partial reliable data transfer.

Table of Contents

1.	Introduction	3
2.	Conventions	4
3.	DTLS considerations	4
4.	SCTP considerations	5
5.	IANA Considerations	5
6.	Security Considerations	5
7.	Acknowledgments	5
8.	References	6
8.1.	Normative References	6
8.2.	Informative References	6
	Authors' Addresses	6
	Intellectual Property and Copyright Statements	8

Internet-Draft

DTLS for SCTP

November 2007

[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](#) [\[RFC0793\]](#).

TLS over SCTP as described in [\[RFC3436\]](#) has some serious limitations:

- o It does not support the unordered delivery of SCTP user messages.
- o It does not support partial reliability as defined in [\[RFC3758\]](#).
- o It only supports the usage of the same number of streams in both directions.
- o 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 endpoints 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 keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [[RFC2119](#)].

[3.](#) DTLS considerations

[3.1.](#) 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.

[3.2.](#) Message sizes

DTLS imposes a limit in the user message size. This limit applies also to DTLS/SCTP.

[3.3.](#) Replay detection

Replay detection of DTLS MUST not be used.

[3.4.](#) Changing of Cipher Specs

Whenever Cipher Specs are changed a new shared secret MUST be derived from the master secret and used for SCTP-AUTH. The shared key

identifier used by SCTP-AUTH MUST be incremented.

[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.](#) Handling of endpoint-pair shared secrets

The endpoint-pair shared secret for Shared Key Identifier 0 is empty. After DTLS cipher specs are changed, a 64 byte shared secret is derived from the master secret and used as the new end-point pair shared secret by using the algorithm described in [\[I-D.rescorla-tls-extractor\]](#). The shared Key identifier MUST be incremented by 1. If it is 65535, the next value MUST be 1.

[5.](#) IANA Considerations

This section is not complete yet.

[6.](#) Security Considerations

This section is not complete yet.

[7.](#) Acknowledgments

The authors wish to thank Carsten Hohendorf for his 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.rescorla-tls-extractor]
Rescorla, E., "Keying Material Extractors for Transport Layer Security (TLS)", [draft-rescorla-tls-extractor-00](#) (work in progress), January 2007.

[8.2](#). Informative References

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

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", [RFC 2246](#), January 1999.

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

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

Authors' Addresses

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

Email: tuexen@fh-muenster.de

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

Email: ekr@networkresonance.com

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).