Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 22, 2008

J. Fischl
CounterPath Solutions, Inc.
H. Tschofenig

November 19, 2007

Session Description Protocol (SDP) Indicators for Datagram Transport Layer Security (DTLS)
draft-fischl-mmusic-sdp-dtls-04.txt

Status of this Memo

Copyright Notice

Abstract

This specification defines how to use the Session Description Protocol (SDP) to signal that media will be transported over Datagram Transport Layer Security (DTLS) or where the SRTP security context is established using DTLS and. It reuses the syntax and semantics for an SDP 'fingerprint' attribute that identifies the certificate which will be presented during the DTLS handshake.

Table of Contents

1. Introduction 3
2. Terminology 3
3. DTLS Certificates 3
4. SDP 4
5. Session Description for RTP/SAVP over DTLS 4
6. IANA Considerations 5
7. Security Considerations 5
8. Acknowledgments 5
9. References 6
9.1. Normative References 6
9.2. Informational References 7
Authors' Addresses 7
Intellectual Property and Copyright Statements 8

1. Introduction

Session Description Protocol (SDP) RFC 2327 [6] has been used to set up the transport of various types of media with RTP [8] over UDP [9], TCP [14], and TLS [12]. DTLS [11] is a protocol for applying TLS security to datagram protocols such as UDP and DCCP [1]. This specification defines new SDP protocol syntax that allow SDP to indicate that DTLS should be used to transport the media when TLS is used.

The handling of TLS sessions in SDP is defined in [12] that discusses only TLS over TCP. This document extends that specification to also deal with TLS over datagram protocols such as UDP and DCCP and when (D)TLS is used to establish keys for SRTP as in [4]

[[NOTE: This document has a major dependency on work currently going on in the MMUSIC WG to mechanisms for SDP capability negotiation which will enable this sort of best-effort encryption. When that work is finished, this draft will be harmonized with it. Furthermore, the contents of this document will be integrated into [4]]]

2. 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 [5].

3. DTLS Certificates

The two endpoints in the exchange present their identities as part of the DTLS handshake procedure using certificates. This document uses certificates in the same style as described in Comedia over TLS in SDP [12].

If self-signed certificates are used, the content of the subjectAltName attribute inside the certificate MAY use the uniform resource identifier (URI) of the user. This is useful for debugging purposes only and is not required to bind the certificate to one of the communication endpoints. The integrity of the certificate is ensured through the fingerprint attribute in the SDP. The subjectAltName is not an important component of the certificate verification.

If the endpoint is also able to make anonymous sessions, a distinct, unique, self-signed certificate SHOULD be provided for this purpose.

The generation of public/private key pairs is relatively expensive. Endpoints are not required to generate certificates for each session.

The endpoints MAY cache their certificates and reuse them across multiple sessions.

[Editor's Note: Certificate lifetime issues will be discussed in a future draft version.]

4. SDP

In addition to the usual contents of an SDP [13] message, each 'm' line will also contain several attributes as specified in RFC 4145 [10] and [12].

The endpoint MUST use the setup and connection attributes defined in "TCP-Based Media Transport in the SDP" [10]. For the purposes of this specification, a setup:active endpoint will act as a DTLS client and a setup:passive endpoint will act as a DTLS server. The connection attribute indicates whether or not to reuse an existing DTLS association.

A certificate fingerprint is the output of a one-way hash function computed over the distinguished encoding rules (DER) form of the certificate. The endpoint MUST use the certificate fingerprint attribute as specified in [12].

TODO: The MMUSIC working group is currently studying the problem of signalling in SDP the ability/desire to initiate a secure channel rather than an insecure one [2][3]. We need to use those techniques when they are finalized.

5. Session Description for RTP/SAVP over DTLS

This specification defines new tokens to describe the protocol used in SDP "m=" lines. The new values defined for the proto field are:

- When a RTP/SAVP stream is transported over DTLS with DCCP, then the token SHALL be DCCP/TLS/RTP/SAVP.
- When a RTP/SAVP stream is transported over DTLS with UDP, the token SHALL be UDP/TLS/RTP/SAVP.
- When a RTP/SAVP stream is transported over TLS with TCP, the token SHALL be TCP/TLS/RTP/SAVP.
- When media is transported over DTLS with UDP, the token SHALL be UDP/TLS.

- When media is transported over DTLS with DCCP, the token SHALL be DCCP/TLS.

For RTP profiles other than SAVP, a new token should be defined in the form of DCCP/TLS/RTP/xyz, UDP/TLS/RTP/xyz and TCP/TLS/RTP/xyz where xyz is replaced with an appropriate token for that profile.

6. IANA Considerations

This specification updates the "Session Description Protocol (SDP) Parameters" registry as defined in Appendix B of RFC 2327 [6]. Specifically it adds the following values to the table for the "proto" field.

Type	SDP Name	Reference
proto	TCP/TLS/RTP/SAVP	[RFC-XXXX]
	UDP/TLS/RTP/SAVP	[RFC-XXXX]
	DCCP/TLS/RTP/SAVP	[RFC-XXXX]
	UDP/TLS	[RFC-XXXX]
	DCCP/TLS	[RFC-XXXX]

Note to RFC Editor: Please replace RFC-XXXX with the RFC number of this specification.

7. Security Considerations

When using self signed certificates, the signalling protocol used to transport the SDP MUST ensure the integrity of the SDP so that the fingerprint attribute can not be altered. Failure to do this would allow a attacker to insert themselves in the media channel as a man-in-the-middle. A method of ensuring the integrity of the SDP when transporting over the SIP RFC 3261 [7] signalling protocol is described in [15]

8. Acknowledgments

Cullen Jennings contributed substantial text and comments to this document. This document benefitted from discussions with Francois Audet, Nagendra Modadugu, Eric Rescorla, and Dan Wing. Thanks also for useful comments by Flemming Andreasen, Rohan Mahy, David McGrew, and David Oran.

9. References

9.1. Normative References

[1] Kohler, E., "Datagram Congestion Control Protocol (DCCP)", draft-ietf-dccp-spec-13 (work in progress), December 2005.

[2] Andreasen, F., "SDP Capability Negotiation", draft-ietf-mmusic-sdp-capability-negotiation-07 (work in progress), October 2007.

[3] Andreasen, F., "SDP Capability Negotiation: Requirements and Review of Existing Work", draft-ietf-mmusic-sdp-capability-negotiation-reqts-01 (work in progress), March 2007.

[4] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)", draft-ietf-avt-dtls-srtp-01 (work in progress), November 2007.

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

[6] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[7] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[8] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[9] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, July 2003.

[10] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.

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

[12] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006.

9.2. Informational References

[13] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[14] Lazzaro, J., "Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport", RFC 4571, July 2006.

[15] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing an SRTP Security Context using DTLS", June 2006.

Authors' Addresses

Jason Fischl
CounterPath Solutions, Inc.
Suite 300, One Bentall Centre, 505 Burrard Street
Vancouver, BC V7X 1M3
Canada

Phone: +1 604 320-3340
Email: jason@counterpath.com

Hannes Tschofenig

Email: Hannes.Tschofenig@gmx.net

Full Copyright Statement

Intellectual Property

Acknowledgment

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