Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 22, 2015

C. Holmberg
Ericsson
R. Shpount
TurboBridge
June 20, 2015

Using the SDP Offer/Answer Mechanism for DTLS
draft-holmberg-mmusic-sdp-dtls-01.txt

Abstract

This draft defines the SDP offer/answer procedures for negotiating and establishing a DTLS association. The draft also defines the criteria for when a new DTLS association must be established.

Table of Contents

1. Introduction

[RFC5763] defines SDP Offer/Answer procedures for SRTP-DTLS. This draft defines the SDP Offer/Answer [RFC3264] procedures for negotiation DTLS in general, based on the procedures in [RFC5763].

This draft also defines the usage of the SDP 'connection' attribute with DTLS. The attribute is used in SDP offers and answers to explicitly indicate whether a new DTLS association is to be established.

As defined in [RFC5245], when Interactive Connectivity Establishment (ICE) [RFC5245] is used, the ufrag value is changed both when ICE is negotiated, and when ICE restart [RFC5245] occurs. These events do not always require a new DTLS association to be established, but currently there is no way to explicitly indicate in an SDP offer or answer whether a new DTLS association is required. To solve that problem, this draft defines the usage of the SDP 'connection' attribute with DTLS. The attribute is used in SDP offers and answers to explicitly indicate whether a new DTLS association is to be established/re-established. The attribute can be used both with and without ICE.

2. Establishing a new DTLS Association

2.1. General

As defined in [RFC5763], an endpoint MUST indicate (in an offer or answer) that a new DTLS association to established in the following cases:

- The DTLS roles change;
- The fingerprint (certificate) value changes;
- The local transport parameters (IP address and/or port) of at least one endpoint change; or
- If ICE is used and the ufrag value changes, and there is no explicit indication (SDP 'connection' attribute) that a new DTLS association shall not be established;

When a new DTLS association is established, an endpoint MUST use a new set of transport parameters (IP address and port combination).

2.2. ICE Considerations

An ICE restart [RFC5245] does not by default require a new DTLS association to be established. A new DTLS association needs to be established only if or more of the criteria listed in Section 2.1 is fulfilled (e.g. if the local transport paramters change).

As defined in [RFC5763], each ICE candidate associated with a component is treated as being part of the same DTLS association. Therefore, from a DTLS perspective it is not considered a change of local transport parameters when an endpoint switches between those ICE candidates.

2.3. SIP Considerations

When the Session Initiation Protocol (SIP) [RFC3261] is used as the signal protocol for establishing a multimedia session, dialogs [RFC3261] might be established between the caller and multiple callees. This is referred to as forking. If forking occurs, separate DTLS associations MUST be established between the caller and each callee.

3. Abbreviations

TBD

4. 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].

5. SDP Connection Attribute for DTLS

5.1. General

The SDP 'connection' attribute [RFC4145] was originally defined for connection-oriented protocols, e.g. TCP and TLS. This section defines how the attribute is used with DTLS.

A 'connection' attribute value of 'new' indicates that a new DTLS association MUST be established. A 'connection' attribute value of 'existing' indicates that a new DTLS association MUST NOT be established.

When used with DTLS, there is no default value defined for the attribute. Implementations that wish to use the attribute MUST explicitly include it in SDP offers and answers. If an offer or answer does not contain an attribute, other means needs to be used in order for endpoints to determine whether an offer or answer is associated with an event that requires the DTLS association to be re-established.

6. SDP Offer/Answer Procedures

6.1. General

This section defines the SDP offer/answer procedures for using the SDP 'connection' attribute for DTLS. The section also describes how the usage of the SDP 'setup' attribute and the SDP 'fingerprint' attribute [RFC4572] is affected.

The procedures in this section are based on the procedures for SRTP-DTLS [RFC5763], with the addition of usage of the SDP 'connection' attribute.

6.2. Generating the Initial SDP Offer

When the offerer sends the initial offer, and the offerer wants to establish a DTLS association, it MUST insert an SDP 'connection' attribute with a 'new' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4572], and an SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the offer.

If ICE is used, the offerer MUST insert the SDP 'ice-ufrag' and 'ice-pwd' attributes according to the procedures in [RFC5245] in the offer.

6.3. Generating the Answer

If an answerer receives an offer that contains an SDP 'connection' attribute with a 'new' value, the answerer MUST insert a 'new' value in the associated answer. The same applies if the answerer receives an offer that contains an SDP 'connection' attribute with a 'new' value, but the answerer determines (based on the criteria for establishing a new DTLS association) that a new DTLS association is to be established. In addition, the answerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4572], and an SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the answer.

If the answerer does not accept the establishment of the DTLS association, it MUST reject the "m=" lines associated with the suggested DTLS association [RFC3264].

If an answerer receives an offer that contains a 'connection' attribute with an 'existing' value, and if the answerer determines that a new DTLS association does not need to be established, it MUST insert a connection attribute with an 'existing' value in the associated answer. In addition, the answerer MUST insert an SDP 'setup' attribute with a value that does not change the previously negotiated DTLS roles, and an SDP 'fingerprint' attribute with a value that does not change the fingerprint, in the answer.

If the answerer receives an offer that does not contain an SDP 'connection' attribute, the answerer MUST NOT insert a 'connection' attribute in the answer.

If ICE is used, the answerer MUST insert the SDP 'ice-ufrag' and 'ice-pwd' attributes according to the procedures in [RFC5245] in the answer.

If a new DTLS association is to be established, and if the answerer becomes DTLS client, the answerer MUST initiate the procedures for establishing the DTLS association. If the answerer becomes DTLS server, it MUST wait for the offerer to establish the DTLS association.

6.4. Offerer Processing of the SDP Answer

When an offerer receives an answer that contains an SDP 'connection' attribute with a 'new' value, and if the offerer becomes DTLS client, the offerer MUST establish a DTLS association. If the offerer becomes DTLS server, it MUST wait for the answerer to establish the DTLS association.

If the answer contains an SDP 'connection' attribute with an 'existing' value, the offerer will continue using the previously established DTLS association. It is considered an error case if the answer contains a 'connection' attribute with an 'existing' value, and a DTLS association does not exist.

6.5. Modifying the Session

When the offerer sends a subsequent offer, and the offerer wants to establish a new DTLS association, the offerer MUST insert an SDP 'connection' attribute with a 'new' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4572], and an SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the offer.

when the offerer sends a subsequent offer, and the offerer does not want to establish a new DTLS association, if a previously established DTLS association exists, the offerer MUST insert an SDP 'connection' attribute with an 'existing' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute with a value that does not change the previously negotiated DTLS roles, and an SDP 'fingerprint' attribute with a value that does not change the fingerprint, in the offer.

If ICE is used, the offerer MUST insert the SDP 'ice-ufrag' and 'ice-pwd' attributes according to the procedures in [RFC5245] in the subsequent offer.

7. RFC Updates

Here we will add the RFC updates that are needed.

8. Security Considerations

This draft does not modify the security considerations associated with DTLS, or the SDP offer/answer mechanism. The draft simply clarifies the procedures for negotiating and establishing a DTLS association.

9. IANA Considerations

TBD

10. Acknowledgements

Thanks to Justin Uberti, Martin Thomson, Paul Kyzivat and Jens Guballa for providing comments and suggestions on the draft.

11. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from draft-holmberg-mmusic-sdp-dtls-00

o - Editorial changes and clarifications.

12. Normative References

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

[RFC3261] 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.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC5763] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)", RFC 5763, May 2010.

Authors' Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Roman Shpount
TurboBridge
4905 Del Ray Avenue, Suite 300
Bethesda, MD 20814
USA

Phone: +1 (240) 292-6632
Email: rshpount@turbobridge.com