Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 17, 2015

C. Holmberg
Ericsson
R. Shpount
TurboBridge

June 15, 2015

DTLS Association Establishment Using the SDP Offer/Answer Mechanism
draft-holmberg-mmusic-sdp-dtls-00.txt

Abstract

This draft defines the criteria for when a DTLS association needs to be established/re-established, based on an SDP offer/answer transaction. The draft also defines how the SDP 'connection' attribute is used with DTLS to signal to the remote peer whether a new DTLS association needs to established/re-established.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 17, 2015.

Table of Contents

1. Introduction

This draft defines the criteria for when a DTLS association needs to be established/re-established, based on an SDP offer/answer transaction. The draft also defines how the SDP 'connection' attribute is used with DTLS to signal to the remote peer whether a new DTLS association needs to established/re-established.

2. Abbreviations

TBD

3. 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].

4. DTLS Association Re-Establishment Criteria

4.1. General

If an endpoint changes the local transport parameters associated with a DTLS association, the endpoint MUST create a new DTLS association. Section 6 defines the SDP Offer/Answer procedures [RFC3264] associated with that.

NOTE: As described in Section 4.4, when Interactive Connectivity Establishment (ICE) [RFC5245] is used there are specific scenarios where the change of transport parameters do not trigger a re-establishment of the DTLS association.

This section describes other events that require re-establishment of a DTLS association. If such event occur, the endpoint MUST also change the local transport parameters. An endpoint MUST NOT re-establish a DTLS association without also changing the local transport parameters, event if the trigger as such for the re-establishment is not a change of the local transport parameters.

NOTE: In future, if new events that require re-establishment of a DTLS association are found, this section should be updated to cover those events.

4.2. Change of DTLS Role

[RFC5763] defines how the DTLS roles are negotiated using an offer/answer transaction. If DTLS roles associated with the DTLS association have previously been negotiated, and a subsequent offer/answer transaction changes the roles, the DTLS association MUST be re-established.

4.3. Change of Fingerprint

If the certificate fingerprint [REF-TO-BE-ADDED] associated with the DTLS association changes, the DTLS association MUST be re-established.

4.4. ICE Considerations

If Interactive Connectivity Establishment (ICE) [RFC5245] is used, the re-establishment of a DTLS association requires the ICE session to be re-established. Similarly, the re-establishment of an ICE session requires re-establishment of the DTLS association.

When an endpoint wants to re-establish the ICE session, if follows the procedures in [RFC5245]. When the endpoint collects the new set

of ICE candidates, the host candidate(s) MUST be different from the previously used host candidates.

An ICE restart [RFC5245] does not require re-establishment of the DTLS association and the ICE session, even if new host candidates might be taken into use due to the restart.

Note that, 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 endpoints switch between those ICE candidates, and hence such switch will not trigger re-establishment of the DTLS association.

NOTE: The procedures defined in [RFC5763] are defined for SRTP-DTLS [RFC5763]. However, this document refer the the procedures for general usage with DTLS.

4.5. 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.

5. SDP Connection Attribute for DTLS

5.1. General

The SDP 'connection' attribute 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 the existing DTLS association MUST be used.

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.

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 to 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.

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 local events) that the DTLS association is to be re-established. In addition, the answerer MUSTbinsert 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 (or re-establishment) of the DTLS association, it MUST reject the offer [RFC3264].

If an answerer receives an offer that contains a 'connection' attribute with an 'existing' value, and if the answerer determines that the DTLS association does not need to be re-established, it MUST insert 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 the DTLS association is to be established (or re-established), and if the answerer becomes DTLS client, the answerer MUST initiate the procedures for establishing/re-establishing the DTLS association. If the answerer becomes DTLS server, it waits for the offerer to establish (or re-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/re-establish the DTLS association. If the offerer becomes DTLS server, it waits for the answerer to establish/ re-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 a previously established DTLS association is to be established (or re-established), 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 DTLS association is not to be established (or re-established), 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.

7. RFC Updates

Here we will add the RFC updates that are needed.

8. Security Considerations

TBD

9. IANA Considerations

TBD

10. Acknowledgements

TBD

11. Change Log

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

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.

[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