Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

C. Holmberg
Ericsson
R. Shpount
TurboBridge

October 19, 2015

Using the SDP Offer/Answer Mechanism for DTLS
draft-ietf-mmusic-dtls-sdp-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.

This draft defines a new SDP media-level attribute, 'dtls-connection'.

Status of This Memo

This Internet-Draft will expire on April 21, 2016.

Copyright Notice

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 a new SDP attribute, 'dtls-connection'. The attribute is used in SDP offers and answers to explicitly indicate whether a new DTLS association is to be established.

As defined in [RFC5763], a new DTLS association MUST be established when transport parameters are changed. Transport parameter change is not well defined when Interactive Connectivity Establishment (ICE)

[RFC5245] is used. One possible way to determine a transport change is based on ufrag change, but 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 a new SDP attribute, 'dtls-connection'. 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. 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. Establishing a new DTLS Association

4.1. General

A new DTLS association MUST be established in the following cases:

o The DTLS roles change;

o The fingerprint (certificate) value changes; or

o The establishment of a new DTLS association is explicitly signaled;

NOTE: The first two items list above are based on the procedures in [RFC5763]. This draft adds the support for explicit signaling.

The sections below describe typical cases where a new DTLS association needs to be established.

4.2. Change of Local Transport Parameters

If an endpoint modifies its local transport parameters (IP address and/or port), and if the modification requires a new DTLS association, the endpoint MUST either change its DTLS role, its fingerprint value and/or use the SDP 'dtls-connection' attribute with a 'new' value Section 5.

4.3. Change of ICE ufrag value

If an endpoint uses ICE, and modifies a local ufrag value, and if the modification requires a new DTLS association, the endpoint MUST either change its DTLS role, its fingerprint value and/or use the SDP 'dtls-connection' attribute with a 'new' value Section 5.

4.4. Multiple SDP fingerprint attributes

It is possible to associate multiple SDP fingerprint attribute values to an 'm-' line. If any of the attribute values associated with an 'm-' line are removed, or if any new attribute values are added, it is considered a fingerprint value change.

5. SDP DTLS-Connection Attribute

5.1. General

The SDP 'connection' attribute [RFC4145] was originally defined for connection-oriented protocols, e.g. TCP and TLS. This section defines a similar attribute, 'dtls-connection', to be used with DTLS.

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

Unlike the SDP 'connection' attribute for TLS, there is no default value defined for the 'dtls-connection' 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.

The SDP Offer/Answer [RFC3264] procedures associated with the attribute are defined in Section 6

5.2. ABNF

The ABNF [RFC5234] grammar for the SDP 'dtls-connection' attributes is:

```
    dtls-connection-attr   = "a=dtls-connection:" conn-value
    conn-value             = "new" / "existing"
```

6. SDP Offer/Answer Procedures

6.1. General

This section defines the SDP offer/answer procedures for using the SDP 'dtls-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 'dtls-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 'dtls-connection' attribute with a 'new' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], and an SDP 'fingerprint' attribute according to the procedures in [RFC4572], in the offer.

Unlike for TCP and TLS connections, in case of DTLS associations the SDP 'setup' attribute 'holdconn' value MUST NOT be used.

6.3. Generating the Answer

If an answerer receives an offer that contains an SDP 'dtls-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 'dtls-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 [RFC4145], 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 'dtls-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 'dtls-connection' attribute, the answerer MUST NOT insert a 'dtls-connection' attribute 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 'dtls-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 'dtls-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 'dtls-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 'dtls-connection' attribute with a 'new' value in the offer. In addition, the offerer MUST insert an SDP 'setup' attribute according to the procedures in [RFC4145], 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 'dtls-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. ICE Considerations

An ICE restart [RFC5245] does not by default require a new DTLS association to be established.

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.

8. 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.

It is possible to send an INVITE request which does not contain an SDP offer. Such INVITE request is often referred to as an 'empty INVITE', or an 'offerless INVITE'. The receiving endpoint will include the SDP offer in a response associated with the response. When the endpoint generates such SDP offer, it MUST assign an SDP connection attribute, with a 'new' value, to each 'm-' line that describes DTLS protected media. If ICE is used, the endpoint MUST allocate a new set of ICE candidates, in order to ensure that two DTLS association would not be running over the same transport.

9. RFC Updates

Here we will add the RFC updates that are needed.

10. 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.

11. IANA Considerations

11.1. Registration of New SDP Attribute

This document updates the "Session Description Protocol Parameters" registry as specified in Section 8.2.2 of [RFC4566]. Specifically,

it adds the SDP attributes in Section 11.1 to the table for SDP media level attributes.

```
Attribute name: dtls-connection
Type of attribute: media-level
Subject to charset: no
Purpose: TBD
Appropriate Values: see Section X
Contact name: Christer Holmberg
```

12. Acknowledgements

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

13. Change Log

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

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

o - SDP 'connection' attribute replaced with new 'dtls-connection' attribute.

o - IANA Considerations added.

o - E-mail regarding 'dtls-connection-id' attribute added as Annex.

Changes from draft-holmberg-mmusic-sdp-dtls-01

o - draft-ietf-mmusic version of draft submitted.

o - Draft file name change (sdp-dtls -> dtls-sdp) due to collision with another expired draft.

o - Clarify that if ufrag in offer is unchanged, it must be unchanged in associated answer.

o - SIP Considerations section added.

o - Section about multiple SDP fingerprint attributes added.

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

o - Editorial changes and clarifications.

14. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, DOI 10.17487/RFC3264, June 2002, <http://www.rfc-editor.org/info/rfc3264>.

[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, DOI 10.17487/RFC4145, September 2005, <http://www.rfc-editor.org/info/rfc4145>.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, DOI 10.17487/RFC4566, July 2006, <http://www.rfc-editor.org/info/rfc4566>.

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, DOI 10.17487/RFC4572, July 2006, <http://www.rfc-editor.org/info/rfc4572>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, DOI 10.17487/RFC5245, April 2010, <http://www.rfc-editor.org/info/rfc5245>.

[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, DOI 10.17487/RFC5763, May 2010, <http://www.rfc-editor.org/info/rfc5763>.

Appendix A. Design Considerations

A.1. dtls-connection versus dtls-connection-id

The text below is from an e-mail sent by Roman to the MMUSIC mailing list, 1st October 2015. It is intended to serve as background reading when discussing the way forward regarding the SDP attribute.

The "dtls-ufrag" has little to do with ICE and exists in a completely different layer. We can call this attribute "dtls-connection-id" if this will makes it less spooky. The problem that I am trying to resolve with new attribute is related to when new DTLS association needs to be established. I would argue that original intent was, that new DTLS association needs to be established on change of one of the end points or DTLS association setup attributes (setup role or fingerprint).

Originally, end point change was detected based on transport 5-tuple change. This, of cause, does not work for ICE, where 5-tuple is not known in advance and all 5-tuples associated with the same ICE component should be treated as the same connection. One option was to detect end point change when ICE is used based on ICE ufrag change, but this does not work either since ufrag can change due to ICE restart, but the same endpoints will continue to communicate.

I would also argue that setting up new DTLS association on 5-tuple change does not always work for non-ICE case either, since we can have an end point which can initiate a re-INVITE when it detects the local IP changes due to DHCP lease expiration or any other reason. This transport change does not necessarily require DTLS association change, and new DTLS handshake is undesirable since it will delay the media flow re-establishment but several network round trips.

So, we need to detect when two new end-points are communicating and new DTLS association needs to be

setup. What we originally proposed is that end point will simply tell that it is setting up a new session by using SDP connection attribute or some renamed version of it.

What I am saying here is that end point cannot always identify if it needs to setup a new DTLS association. The problem arises when new offer is generated in response to an offerless INVITE. In such case, an end point does not know if it is continuing to communicate with the same end-point or if this offer is intended to be sent to a new end point.

There are two solution possible to this:

1. We specify that if an end points generates an offer in response to an offer-less INVITE it should always assume it is communicating with a new end point, it MUST add "connection:new" and MUST make sure that none of the existing transports can be possibly reused for this new DTLS association by allocating new IP:port for non ICE or a complete new set of ICE candidates in case of ICE. This will work, but it is wasteful when offer-less INVITE re-establishes connection between two existing end points. In such cases additional ports will be consumed, TURN tunnels will be allocated, and time spent on creating a DTLS session when all of this can be simply reused.

2. Instead of asking the end point which generates the offer to determine if it is establishing a new DTLS association, we will ask the end point to identify itself. So, instead of SDP connection attribute, an end point will provide some sort of randomly generated end point identifier in the new attribute (dtls-ufrag or dtls-connection-id). When the connection ID pair stays the same, the existing DTLS association continues to run over the negotiated transport. If one of the connection IDs changes, this would mean new DTLS association would need to be established. This nicely uncouples end point change identification from transport and makes negotiation follow the original intent.

In case of response to an offer-less INVITE, an offer with the existing connection ID will be generated. If this offer is sent to a new end point, both end points will detect that new DTLS association is required due to connection ID change of the answering end point. If this offer will be sent to an end point which is already a part of the existing

DTLS association, no new DTLS association will be necessary, since both connection IDs will stay the same.

This also gives us path to a more "strategic" solution in the future. DTLS handshake can be extended to include the connection ID. Each DTLS handshake can negotiate a association identifier similar to SSRC which can be used in the all subsequent DTLS messages for this association. This way multiple DTLS associations can be multiplexed over the single transport and each of them can be tied to an m= line in offer/answer. This, of cause, is not part of the current draft and is outside of MMUSIC chapter, but does provide a natural extension path for DTLS in the future.

In general Christer and I are trying to understand if there is interest in formalizing the dtls-connection-id option (more complex) or if we should stick with SDP connection:new/existing attribute and force new DTLS association always be established in response to offer-less INVITE (simpler option but can waste resources).

Please let us know if these options need further clarification or if you have any additional questions or opinions.

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