Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

P. Jones
Cisco Systems
N. Ohlmeier
Mozilla

March 13, 2017

Transporting the SDP attribute 'dtls-id' in TLS and DTLS
draft-jones-perc-dtls-id-00

Abstract

This draft defines a new extension to carry the "dtls-id" value defined for use in the Session Description Protocol within TLS and DTLS.

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 September 14, 2017.

Table of Contents

1. Introduction

The Privacy-Enhanced RTP Conferencing (PERC) working group specified a DTLS [RFC6347] tunneling mechanism [I-D.ietf-perc-dtls-tunnel] that enables a media distributor to forward DTLS messages between an endpoint and a key distributor. In the process, the media distributor is able to securely receive only the hop-by-hop keying material, while the endpoints are able to securely receive both end-to-end and hob-by-hop keying material.

An open issue with the current design is how the key distributor can determine which one of several conferences an endpoint is attempting to join. The only information that the key distributor receives via the DTLS tunnel is the endpoint's certificate. However, the same certificate might be used to join several conferences in parallel, thus creating a need for additional information.

[I-D.ietf-mmusic-dtls-sdp] defines an attribute in SDP [RFC4566] called the "dlts-id". The "dtls-id" presented by the endpoint's in SDP will be unique for each DTLS association established using the same certificate. By signaling the certificate fingerprint and "dtls-id" in SDP, along with including the same in the DTLS signaling sent to the key distributor, it would be possible for the key distributor to unambiguously determine which conference key the endpoint should receive.

2. Conventions Used In This Document

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] when they appear in ALL CAPS. These words may also appear in this document in lower case as plain English words, absent their normative meanings.

The terms key distributor, media distributor, endpoint, conference, hop-by-hop keying material, and end-to-end keying material used in this document are introduced in [I-D.ietf-perc-private-media-framework].

3. Endpoint procedures

The endpoint MUST include the "dtls_id" DTLS extension in the "ClientHello" message when establishing a DTLS tunnel in a PERC conference. Likewise, the "dtls-id" SDP attribute MUST be included in SDP sent by the endpoint in both the offer and answer [RFC3264] messages as per [I-D.ietf-mmusic-dtls-sdp].

When receiving a "dtls_id" value from the key distributor, the client MUST check to ensure that value matches the "dtls-id" value received in SDP. If the values do not match, the endpoint MUST consider any received keying material to be invalid and terminate the DTLS association.

4. Media distributor procedures

The media distributor is not required to inspect the "dtls_id" extension, as it merely forwards DTLS messages between the endpoint and the key distributor.

5. Key distributor procedures

This draft assumes that when the endpoint inserts the "dtls-id" into SDP, the information will be conveyed in some way to the key distributor. The process through which the "dtls-id" in SDP is conveyed to the key distributor is outside the scope of this document.

The key distributor MUST extract the "dtls_id" value transmitted in the "ClientHello" message and match that against "dtls-id" value the endpoint transmitted via SDP. If the values in SDP and the "ClientHello" do not match, the DTLS association MUST be rejected.

The key distributor MUST correlate the certificate fingerprint and "dtls_id" received from endpoint's "ClientHello" message with the corresponding values received from the SDP transmitted by the endpoint. It is through this correlation that the key distributor can be sure to deliver the correct conference key to the endpoint.

When sending the "ServerHello" message, the key distributor MUST insert its own "dtls-id" value. This value MUST also be conveyed back to the client via SDP.

6. The dtls_id TLS extension

The "dtls_id" TLS extension may be used either with TLS [RFC5246] or DTLS. It carries only "dtls-id" value defined in [I-D.ietf-mmusic-dtls-sdp] in the field called "dtls_id". The syntax for the "dtls_id" extension is shown below.

```
struct {
    opaque dtls_id<20..255>;
} SdpDtlsIdData;
```

7. IANA Considerations

This document registers an extension in the TLS "ExtensionType Values" registry established in [RFC5246]. The extension is called "dtls_id" and is assigned the code point TBD. The following addition is made to the registry.

Extension	Recommended	TLS 1.3	HelloRetryRequested
dlts_id	Yes	Encrypted	Yes

8. Security Considerations

The "dtls-id" value is a random value that has no personal identifiable information associated with it. Thus, the value does not expose such information. It also has no particular security properties in and of itself, so being in plaintext in the "ClientHello" or "ServerHello" is not viewed as a security concern.

However, the value does have significance to the receiver, thus changes to the "dtls-id" may result in unexpected behavior. For example, if Alice attempts to join a PERC-enabled conference and the "dtls_id" field is modified in route to the key distributor, Alice may either fail to receive the conference key or receive the wrong conference key. However, since Alice will only be provided keys for conferences for which she is authorized to join based on her client certificate, receiving the wrong key will not compromise the security of the conference. However, receipt of the wrong key will deny Alice access to the plaintext of media transmitted by other participants. Additionally, if Alice transmits media using the wrong conference key, the media will be undecipherable by other conference participants.

As prescribed in these procedures, if the "dtls_id" field transmitted from the key distributor to Alice is modified, Alice will tear down

the DTLS association and fail to join the conference. The result is a denial of service for Alice, but not worse than when any other part of the DTLS message is modified.

9. Acknowledgments

The authors would like to thank Martin Thomson for discussing the idea and providing some initial feedback before the draft was written. We also want to express our appreciation to Cullen Jennings for reviewing the text and providing constructive input.

10. Normative References

[I-D.ietf-mmusic-dtls-sdp]
Holmberg, C. and R. Shpount, "Using the SDP Offer/Answer Mechanism for DTLS", draft-ietf-mmusic-dtls-sdp-20 (work in progress), February 2017.

[I-D.ietf-perc-dtls-tunnel]
Jones, P., Ellenbogen, P., and N. Ohlmeier, "DTLS Tunnel between a Media Distributor and Key Distributor to Facilitate Key Exchange", draft-ietf-perc-dtls-tunnel-00 (work in progress), March 2017.

[I-D.ietf-perc-private-media-framework]
Jones, P., Benham, D., and C. Groves, "A Solution Framework for Private Media in Privacy Enhanced RTP Conferencing", draft-ietf-perc-private-media-framework-02 (work in progress), October 2016.

[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>.

[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>.

[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>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

Authors' Addresses

Paul E. Jones
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, North Carolina 27709
USA

Phone: +1 919 476 2048
Email: paulej@packetizer.com

Nils H. Ohlmeier
Mozilla

Phone: +1 408 659 6457
Email: nils@ohlmeier.org