Abstract

Session Initiation Protocol (SIP) Back-to-Back User Agents (B2BUAs) often act on the media plane, rather than just on the signaling path. This document describes the behavior such B2BUAs can adhere to when acting on the media plane that uses a Secure Real-time Transport (SRTP) security context set up with the Datagram Transport Layer Security (DTLS) protocol.
1. Introduction

1.1. Overview

[RFC5763] describes how Session Initiation Protocol (SIP) [RFC3261] can be used to establish a Secure Real-time Transport Protocol (SRTP) [RFC3711] security context with the Datagram Transport Layer Security (DTLS) [RFC6347] protocol. It describes a mechanism for transporting a certificate fingerprint using Session Description Protocol (SDP) [RFC4566]. The fingerprint, identifies the certificate that will be presented during the DTLS handshake. DTLS-SRTP is defined for point-to-point media sessions, in which there are exactly two participants. Each DTLS-SRTP session (described in Section 3 of [RFC5764]) contains a single DTLS connection (if RTP and RTCP are multiplexed) or two DTLS connections (if RTP and RTCP are not multiplexed), and either two SRTP contexts (if media traffic is flowing in both directions on the same 5-tuple) or one SRTP context (if media traffic is only flowing in one direction).
In many SIP deployments, SIP Back-to-Back User Agents (B2BUA) entities exist on the SIP signaling path between the endpoints. As described in [RFC7092], these B2BUAs can modify SIP and SDP information. They can also be present on the media path, in which case they modify parts of the SDP information (like IP address, port) and subsequently modify the RTP headers as well. Such B2BUAs are referred to as media plane B2BUAs.

1.2. Goals

[RFC7092] describes two different categories of media plane B2BUAs, according to the level of activities performed on the media plane:

A B2BUA that acts as a simple media relay effectively unaware of anything that is transported and only terminates the media plane at the IP and transport (UDP/TCP) layers.

A B2BUA that performs a media-aware role. It inspects and potentially modifies RTP headers or RTP Control Protocol (RTCP) packets.

The following sections describe the behavior B2BUAs MUST follow in order to avoid any impact to end-to-end DTLS-SRTP sessions.

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 [RFC2119].

The following generalized terms are defined in [RFC3261], Section 6.

B2BUA: a SIP Back-to-Back User Agent, which is the logical combination of a User Agent Server (UAS) and User Agent Client (UAC).

UAS: a SIP User Agent Server.

UAC: a SIP User Agent Client.

All of the pertinent B2BUA terminology and taxonomy used in this document is based on [RFC7092].

It is assumed the reader is already familiar with the fundamental concepts of the RTP protocol [RFC3550] and its taxonomy [I-D.ietf-avtext-rtp-grouping-taxonomy], as well as those of SRTP [RFC3711], and DTLS [RFC6347].
3. Media Plane B2BUA Handling of DTLS-SRTP

3.1. General

This section describes the DTLS-SRTP handling by the different types of media plane B2BUAs defined in [RFC7092].

3.1.1. Media Relay

A media relay, as defined in section 3.2.1 of [RFC7092], from an application layer point-of-view, forwards all packets it receives on a negotiated connection, without inspecting or modifying the packet contents. A media relay only modifies the transport layer (UDP/TCP) and IP headers.

A media relay B2BUA MUST forward the certificate fingerprint and SDP setup attribute it receives from one endpoint unmodified towards the other endpoint and vice-versa. The example below shows a SIP call establishment flow, with both SIP endpoints (user agents) using DTLS-SRTP, and a media relay B2BUA.
NOTE: For brevity the entire value of the SDP fingerprint attribute is not shown. The example here shows only one DTLS connection for the sake of simplicity. In reality depending on whether the RTP and RTCP flows are multiplexed or demultiplexed there will be one or two DTLS connections.

If RTP and RTCP traffic is multiplexed as described in [RFC5761] on a single port then only a single DTLS connection is required between the peers. If RTP and RTCP are not multiplexed, then the peers would
have to establish two DTLS connections. In this case, Bob, after he receives an INVITE request, triggers the establishment of a DTLS connection. Note that the DTLS handshake and the sending of an INVITE response can happen in parallel; thus, the B2BUA SHOULD be prepared to receive DTLS, STUN and media on the ports it advertised to Bob in the INVITE request. Since a media relay B2BUA does not differentiate between a DTLS message, RTP or any packet it receives, it only changes the transport layer (UDP/TCP) and IP headers and forwards the packet towards the other endpoint. B2BUA cannot decrypt the RTP payload as the payload is encrypted using the SRTP keys derived from the DTLS connection setup between Alice and Bob.

[I-D.ietf-stir-rfc4474bis] provides a means for signing portions of SIP requests in order to provide identity assurance and certificate pinning by providing a signature over the fingerprint of keying material in SDP for DTLS-SRTP [RFC5763]. A media relay B2BUA MUST ensure that it does not modify any of the information used to construct the signature.

In the above example, Alice can be authorized by the authorization server (SIP proxy) in its domain using the procedures in Section 5 of [I-D.ietf-stir-rfc4474bis]. In such a case, if the B2BUA modifies some of the SIP headers or SDP content that was used by Alice’s authorization server to generate the identity, it would break the identity verification procedure explained in Section 4.2 of [I-D.ietf-stir-rfc4474bis] resulting in a 438 error response being returned.

3.1.2. RTP/RTCP-aware Media Aware B2BUA

Unlike the media relay discussed in Section 3.1.1, a media-aware relay as defined in Section 3.2.2 of [RFC7092], is aware of the type of media traffic it is receiving. There are two types of media-aware relay, those that merely inspect the RTP headers and RTCP packets, and those that inspect and modify the RTP headers and RTCP packets. The mechanism described in Security Considerations section MUST be used by endpoint to detect malicious B2BUA’s that MAY attempt to terminate the DTLS-SRTP session.

3.1.2.1. RTP header and RTCP packets Inspection

This kind of media aware relay does not modify the RTP headers and RTCP packets but only inspects the packets. It MUST NOT terminate the DTLS-SRTP session on which the packets are received.
3.1.2.2. RTP header and RTCP packet Modification

In order to modify headers a B2BUA needs to act as a DTLS endpoint and terminate the DTLS-SRTP session and decrypt/re-encrypt RTP payload. This would break end-to-end security and hence a B2BUA MUST NOT terminate DTLS-SRTP session. This security and privacy problem can be mitigated by having different keys for protecting RTP header integrity and encrypting the RTP payload. For example, the approach discussed in [I-D.jones-perc-private-media-reqts] can be used. With such an approach, the B2BUA is not aware of the keys used to decrypt the media payload.

3.2. Media Plane B2BUA with NAT Handling

DTLS-SRTP handshakes and SDP offer/answer exchanges [RFC3264] may happen in parallel. If an endpoint is behind a NAT, and the endpoint is acting as a DTLS server, the ClientHello message from a B2BUA (acting as DTLS client) is likely to be lost, as described in Section 7.3 of [RFC5763]. In order to overcome this problem, the endpoint and B2BUA can support the Interactive Connectivity Establishment (ICE) mechanism [RFC5245], as discussed in Section 7.3 of [RFC5763]. If the ICE check is successful then the endpoint will receive the ClientHello message from the B2BUA.

4. Forking Considerations

Due to forking [RFC3261], a SIP request carrying an SDP offer sent by an endpoint (offerer) can reach multiple remote endpoints. As a result, multiple DTLS-SRTP sessions can be established, one between the endpoint that sent the SIP request and each of the remote endpoints that received the request. Both media relays and media-aware relays MUST forward the certificate fingerprints and SDP setup attributes it received in the SDP answer from each endpoint (answerer) unmodified towards the offerer. Since DTLS operates on the 5-tuple, B2BUA MUST replace the answerer’s transport addresses in each answer with its unique transport addresses so that the offerer can establish a DTLS connection with each answerer.
Bob (192.0.2.1:6666) / / DTLS-SRTP=XXX / / DTLS-SRTP=XXX v
<----------->  (192.0.2.3:7777)
Alice (192.0.2.0:5555)  B2BUA
<----------->  (192.0.2.3:8888)
DTLS-SRTP=YYY ^
\ DTLS-SRTP=YYY \ \ \ \ 
| Charlie (192.0.2.2:6666)
Figure 2: B2BUA handling multiple answers

For instance, as shown in Figure 2 Alice sends a request with an offer, and the request is forked. Alice receives answers from both Bob and Charlie. B2BUA MUST advertise different B2BUA transport address in each answer, as shown in Figure 2, where XXX and YYY represent different DTLS-SRTP sessions. B2BUA replaces the Bob’s transport address (192.0.2.1:6666) in the answer with its transport address (192.0.2.3:7777) and Charlie’s transport address (192.0.2.2:6666) in the answer with its transport address (192.0.2.3:8888). B2BUA tracks the remote sources (Bob and Charlie) and associates them to the local sources that are used to send packets to Alice.

5. Security Considerations

This document describes the behavior media plane B2BUAs (media-aware and media-unaware) MUST follow when acting on the media plane that uses SRTP security context setup with the DTLS protocol. Attempting to cover media-aware relay modifying RTP headers and media termination scenarios involving secure sessions (like DTLS-SRTP) will inevitably lead to the B2BUA acting as a man-in-the-middle, and hence a B2BUA MUST NOT terminate DTLS-SRTP session. This document does not introduce any specific security considerations beyond those detailed in [RFC5763]. In addition, the B2BUA behaviors outlined in this document do not impact the security and integrity of a DTLS-SRTP session or the data exchanged over it. A malicious B2BUA MAY try to break into the DTLS connection, but such an attack can be prevented using the identity validation mechanism discussed in [RFC4474] and getting updated in [I-D.ietf-stir-rfc4474bis]. Either the endpoints
or authentication service proxies involved in the call MUST use the identity validation mechanisms discussed in [RFC4474] to validate the identity of peers and detect malicious B2BUA’s that can attempt to terminate the DTLS connection to decrypt the RTP payload.

6. IANA Considerations

This document makes no request of IANA.

7. Acknowledgments

Special thanks to Lorenzo Miniero, Ranjit Avarsala, Hadriel Kaplan, Muthu Arul Mozhi, Paul Kyzivat, Peter Dawes, Brett Tate, Dan Wing, Charles Eckel, Simon Perreault, Albrecht Schwarz, Jens Guballa, Christer Holmberg and Colin Perkins for their constructive comments, suggestions, and early reviews that were critical to the formulation and refinement of this document.

8. Contributors

Rajeev Seth provided substantial contributions to this document.

9. References

9.1. Normative References


9.2. Informative References

[I-D.ietf-avtext-rtp-grouping-taxonomy]

[I-D.ietf-stir-rfc4474bis]

[I-D.jones-perc-private-media-reqts]


Authors’ Addresses

Ram Mohan Ravindranath
Cisco
Cessna Business Park
Sarjapur-Marathahalli Outer Ring Road
Bangalore, Karnataka  560103
India

Email: rmohanr@cisco.com

Tirumaleswar Reddy
Cisco
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka  560103
India

Email: tireddy@cisco.com