SIPBRANDY Working Group
Internet-Draft
Intended status: Informational
Expires: September 16, 2018

A. Johnston
Rowan University
B. Aboba
Microsoft
A. Hutton
Atos
R. Jesske
Deutsche Telekom
T. Stach
Unaffiliated

March 15, 2018

An Opportunistic Approach for Secure Real-time Transport Protocol (OSRTP)
draft-ietf-sipbrandy-osrtp-04

Abstract

Opportunistic Secure Real-time Transport Protocol (OSRTP) is an implementation of the Opportunistic Security mechanism, as defined in RFC 7435, applied to Real-time Transport Protocol (RTP). OSRTP allows encrypted media to be used in environments where support for encryption is not known in advance, and not required. OSRTP does not require SDP extensions or features and is fully backwards compatible with existing implementations using encrypted and authenticated media and implementations that do not encrypt or authenticate media packets. OSRTP is not specific to any key management technique for SRTP. OSRTP is a transitional approach useful for migrating existing deployments of real-time communications to a fully encrypted and authenticated state.

Copyright Notice

Table of Contents

1. Introduction

Opportunistic Security [RFC7435] (OS) is an approach to security that defines a third mode for security between "cleartext" and "comprehensive protection" that allows encryption and authentication to be used if supported but will not result in failures if it is not supported. In terms of secure media, cleartext is RTP [RFC3550] media which is negotiated with the RTP/AVP (Audio Video Profile) profile defined [RFC3551]. Comprehensive protection is Secure RTP [RFC3711], negotiated with a secure profile, such as SAVP or SAVPF [RFC5124]. OSRTP allows SRTP to be negotiated with the RTP/AVP profile, with fallback to RTP if SRTP is not supported.

There have been some extensions to SDP to allow profiles to be negotiated such as SDP Capabilities Negotiation (capneg) [RFC5939] . However, these approaches are complex and have very limited deployment in communication systems. Other key management protocols for SRTP have been developed which by design use OS, such as ZRTP [RFC6189]. This approach for OSRTP is based on

[I-D.kaplan-mmusic-best-effort-srtp] where it was called "best effort SRTP". [I-D.kaplan-mmusic-best-effort-srtp] has a full discussion of the motivation and requirements for opportunistic secure media.

OSRTP uses the presence of SRTP keying-related attributes in an SDP offer to indicate support for opportunistic secure media. The presence of SRTP keying-related attributes in the SDP answer indicates that the other party also supports OSRTP and encrypted and authenticated media will be used. OSRTP requires no additional extensions to SDP or new attributes and is defined independently of the key agreement mechanism used. OSRTP is only usable when media is negotiated using the Offer/Answer protocol [RFC3264].

1.1. Applicability Statement

OSRTP is a transitional approach that provides a migration path from unencrypted communication (RTP) to fully encrypted communication (SRTP). It is only to be used in existing deployments which are attempting to transition to fully secure communications. New applications and new deployments will not use OSRTP.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Definition of Opportunistic Security for SRTP

To indicate support for OSRTP in an SDP offer, the offerer uses the RTP/AVP profile [RFC3551] but includes SRTP keying attributes. OSRTP is not specific to any key management technique for SRTP. For example:

If the offerer supports DTLS-SRTP key agreement [RFC5763], then an a=fingerprint attribute will be present, or

If the offerer supports SDP Security Descriptions key agreement [RFC4568], then an a=crypto attribute will be present, or

If the offerer supports ZRTP key agreement [RFC6189], then an a=zrtp-hash attribute will be present.

To accept OSRTP, an answerer receiving an offer indicating support for OSRTP generates an SDP answer containing SRTP keying attributes which match one of the keying methods in the offer. The answer MUST NOT contain attributes from more than one keying method, even if the

offer contained multiple keying method attributes. The selected SRTP key management approach is followed and SRTP media is used for this session. If the SRTP key management fails for any reason, the media session MUST fail. To decline OSRTP, the answerer generates an SDP answer omitting SRTP keying attributes, and the media session proceeds with RTP with no encryption or authentication used.

If the offerer of OSRTP receives an SDP answer which does not contain SRTP keying attributes, then the media session proceeds with RTP. If the SDP answer contains the RTP/AVP profile with SRTP keying attributes or the SAVP (or UDP/TLS/RTP/SAVP(F)) profile with SRTP keying attributes, then that particular SRTP key management approach is followed and SRTP media is used for this session. If the SRTP key management fails, the media session MUST fail.

It is important to note that OSRTP makes no changes, and has no effect on media sessions in which the offer contains a secure profile of RTP, such as SAVP or SAVPF. As discussed in [RFC7435], this is the "comprehensive protection" for media mode.

4. Security Considerations

The security considerations of [RFC7435] apply to OSRTP, as well as the security considerations of the particular SRTP key agreement approach used. However, the authentication requirements of a particular SRTP key agreement approach are relaxed when that key agreement is used with OSRTP. For example:

For DTLS-SRTP key agreement [RFC5763], an authenticated signaling channel does not need to be used with OSRTP if it is not available.

For SDP Security Descriptions key agreement [RFC4568], an authenticated signaling channel does not need to be used with OSRTP if it is not available, although an encrypted signaling channel must still be used.

For ZRTP key agreement [RFC6189], the security considerations are unchanged, since ZRTP does not rely on the security of the signaling channel.

As discussed in [RFC7435], OSRTP is used in cases where support for encryption by the other party is not known in advance, and not required. For cases where it is known that the other party supports SRTP or SRTP needs to be used, OSRTP MUST NOT be used. Instead, a secure profile of RTP is used in the offer.

5. Implementation Status

Note to RFC Editor: Please remove this entire section prior to publication, including the reference to [RFC6982].

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC6982]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC6982], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

There are implementations of [I-D.kaplan-mmusic-best-effort-srtp] in deployed products by Microsoft and Unify. The IMTC "Best Practices for SIP Security" document [IMTC-SIP] recommends this approach. The SIP Forum planned to include support in the SIPconnect 2.0 SIP trunking recommendation [SIPCONNECT]. There are many deployments of ZRTP [RFC6189].

6. Acknowledgements

This document is dedicated to our friend and colleague Francois Audet who is greatly missed in our community. His work on improving security in SIP and RTP provided the foundation for this work.

Thanks to Eric Rescorla, Martin Thomson, and Richard Barnes for their comments.

7. References

7.1. 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, <https://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, <https://www.rfc-editor.org/info/rfc3264>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, DOI 10.17487/RFC3551, July 2003, <https://www.rfc-editor.org/info/rfc3551>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <https://www.rfc-editor.org/info/rfc3711>.

[RFC4568] Andreasen, F., Baugher, M., and D. Wing, "Session Description Protocol (SDP) Security Descriptions for Media Streams", RFC 4568, DOI 10.17487/RFC4568, July 2006, <https://www.rfc-editor.org/info/rfc4568>.

[RFC5124] Ott, J. and E. Carrara, "Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)", RFC 5124, DOI 10.17487/RFC5124, February 2008, <https://www.rfc-editor.org/info/rfc5124>.

[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, <https://www.rfc-editor.org/info/rfc5763>.

[RFC6189] Zimmermann, P., Johnston, A., Ed., and J. Callas, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", RFC 6189, DOI 10.17487/RFC6189, April 2011, <https://www.rfc-editor.org/info/rfc6189>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

7.2. Informative References

[I-D.kaplan-mmusic-best-effort-srtp]
Audet, F. and H. Kaplan, "Session Description Protocol (SDP) Offer/Answer Negotiation For Best-Effort Secure Real-Time Transport Protocol", draft-kaplan-mmusic-best-effort-srtp-01 (work in progress), October 2006.

[IMTC-SIP]
"Best Practices for SIP Security", IMTC SIP Parity Group http://www.imtc.org/uc/sip-parity-activity-group/, 2011, <http://www.imtc.org>.

[RFC5939] Andreasen, F., "Session Description Protocol (SDP) Capability Negotiation", RFC 5939, DOI 10.17487/RFC5939, September 2010, <https://www.rfc-editor.org/info/rfc5939>.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, DOI 10.17487/RFC6982, July 2013, <https://www.rfc-editor.org/info/rfc6982>.

[SIPCONNECT]
"SIP-PBX / Service Provider Interoperability SIPconnect 2.0 - Technical Recommendation", SIP Forum http://www.sipforum.org/component/option,com_docman/task,doc_download/gid,838/Itemid,261/, 2017, <http://www.sipforum.org>.

Authors' Addresses

Alan Johnston
Rowan University
Glassboro, NJ
USA

Email: alan.b.johnston@gmail.com

Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

Email: bernard.aboba@gmail.com

Andrew Hutton
Atos
4 Triton Square
London NW1 3HG
UK

Email: andrew.hutton@atos.net

Roland Jesske
Deutsche Telekom
Heinrich-Hertz-Strasse 3-7
Darmstadt 64295
Germany

Email: R.Jesske@telekom.de

Thomas Stach
Unaffiliated

Email: thomass.stach@gmail.com