Network Working Group
Internet-Draft
Updates: 4568,4585 (if approved)
Intended status: Standards Track
Expires: December 7, 2017

A. Hutton
Unify
R. Jesske
Deutsche Telekom
A. Johnston
Unaffiliated
G. Salgueiro
Cisco
B. Aboba
Microsoft

June 5, 2017

Negotiating SRTP and RTCP Feedback using the RTP/AVP Profile
draft-ietf-mmusic-opportunistic-negotiation-00

Abstract

This document describes how the use of the Secure Real-time transport protocol (SRTP) [RFC3711]. can be negotiated using the AVP (Audio Video Profile) defined in [RFC3551]. Such a mechanism is used to provide a means for encrypted media to be used in environments where support for encryption is not known in advance, and not required. The same mechanism is also applied to negotiation of the Extended RTP Profile for Real-time Transport Control Protocol Based Feedback (RTP/AVPF) [RFC4585].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Opportunistic Security [RFC7435] 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 AVP (Audio Video Profile) profile defined [RFC3551]. Comprehensive protection is Secure RTP [RFC3711], negotiated with a secure profile, such as SAVP or SAVPF [RFC5124].

[I-D.ietf-sipbrandy-osrtp] describes how Secure Real-time transport protocol (SRTP) can be negotiated opportunistically.

[RFC4568] however requires that SRTP is only negotiated using the RTP/SAVP profile [RFC3711] or the RTP/SAVPF profile [RFC5124]. This document relaxes this rule by allowing SRTP to be used with the RTP/AVP profile when negotiated opportunistically.

Similarly [RFC4585] requires that the RTCP extended reports are only used in media sessions for which the "AVPF" profile is specified. This document therefore also relaxes this rule allowing RTCP based feedback to be used with the RTP/AVP profile.

2. Normative Language

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 BCP 14, RFC 2119 [RFC2119].

3. Motivation

In theory SDP [RFC4566] allows different RTP profiles such as SAVP, AVPF, and AVP to be offered as separate m-lines, and allows the answerer to reject profiles it does not support or does not wish to use. However the use of multiple m-lines for such a negotiation is not well defined and implementations receiving such an offer are likely to reject the SDP Offer rather than use the profile they support. This negotiation failure has been observed when negotiating the secure profile (SAVP) and also when negotiating RTCP based feedback messages [RFC4585] (RTP/AVPF) or both (RTP/SAVPF).

To avoid using multiple m-lines to negotiate RTP profiles this draft recognized that existing implementation of SRTP, and RTCP feedback, make use of the relevant SDP attributes to indicate such capabilities. The approach therefore taken in this draft uses the "a=" lines in SDP to negotiate these capabilities in a single offer/ answer exchange, by offering the AVP profile but indicating the supported functionality in a=lines.

4. Use of RTP/AVP profile with SRTP

To negotiate SRTP in an opportunistic way such as that described in [I-D.ietf-sipbrandy-osrtp] requires a fallback to unencrypted media to occur if the remote endpoint does not support SRTP.

Therefore when negotiating SRTP opportunistically the SDP offerer MUST use the AVP profile [RFC3551]. This is independent of the key exchange mechanism used.

The SDP answerer MUST use the AVP profile if it does not encrypt the media and MAY use the AVP if it encrypts the media. The exact negotiation mechanism is however outside the scope of this document, an example mechanism can be found in [I-D.ietf-sipbrandy-osrtp].

5. Use of RTP/AVP profile with RTCP Feedback

Negotiating the use of the Extended RTP Profile for RTCP Based Feedback (RTP/AVPF) [RFC4585] opportunistically also requires the offerer to use the AVP profile otherwise the offer is likely to be rejected by an answerer who does not support AVPF.

Therefore when negotiating RTCP Based Feedback opportunistically the SDP offerer MUST use the AVP profile [RFC3551] and include the "a=rtcp-fb" SDP attribute as described in [RFC4585].

The SDP answerer indicates support for RTCP Based Feedback by including the "a=rtcp-fb" SDP attribute in the SDP Answer. The RTP profile in the SDP answer MAY be set to AVP (SAVP) or AVPF (SAVPF).

This is an update to [RFC4585] which requires that the "a=rtcp-fb" attribute is only used with the AVPF profile. All other [RFC4585] procedures remain unchanged.

6. IANA Considerations

None

7. Security Considerations

The security considerations of [RFC7435] apply to any opportunistic approach to SRTP.

It is important to note that negotiating SRTP in an opportunistic way 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.

8. 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.

9. References

9.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

9.2. Informative References

[I-D.ietf-sipbrandy-osrtp]
Johnston, A., Aboba, B., Hutton, A., Jesske, R., and T. Stach, "An Opportunistic Approach for Secure Real-time Transport Protocol (OSRTP)", draft-ietf-sipbrandy-osrtp-02 (work in progress), May 2017.

[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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc3711>.

[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>.

[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, <http://www.rfc-editor.org/info/rfc4568>.

[RFC4585] Ott, J., Wenger, S., Sato, N., Burmeister, C., and J. Rey, "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)", RFC 4585, DOI 10.17487/RFC4585, July 2006, <http://www.rfc-editor.org/info/rfc4585>.

[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, <http://www.rfc-editor.org/info/rfc5124>.

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

Authors' Addresses

Andrew Hutton
Unify
Brickhill Street
Milton Keynes MK15 0DJ
UK

Email: andrew.hutton@unify.com

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

Email: R.Jesske@telekom.de

Alan Johnston
Unaffiliated
Bellevue, WA
USA

Email: alan.b.johnston@gmail.com

Gonzalo Salgueiro
Cisco
7200-12 Kit Creek Road
RTP, NC 27709
USA

Email: gsalguei@cisco.com

Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

Email: bernard.aboba@gmail.com