       An Opportunistic Approach for Secure Real-time Transport Protocol
                                (OSRTP)

Abstract

   Opportunistic Secure Real-time Transport Protocol (OSRTP) is an
   implementation of the Opportunistic Security mechanism, as defined in
   RFC 7435, applied to the Real-time Transport Protocol (RTP).  OSRTP
   allows encrypted media to be used in environments where support for
   encryption is not known in advance and is not required.  OSRTP does
   not require Session Description Protocol (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 Secure RTP (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 (OS) [RFC7435] is an approach to security that
   defines a third mode for security between "cleartext" and
   "comprehensive protection" that allows encryption and authentication
   of media to be used if supported but will not result in failures if
   it is not supported.  In the context of the transport of secure media
   streams using RTP and its secured derivatives, cleartext is
   represented by an RTP [RFC3550] media stream that is negotiated with
   the RTP/AVP (Audio-Visual Profile) [RFC3551] or the RTP/AVPF profile
   [RFC4585], whereas comprehensive protection is represented by a
   Secure RTP [RFC3711] stream 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 (SDPCapNeg)
[RFC5939].  However, these approaches are complex and have very
limited deployment in communication systems.  Other key management
protocols for SRTP that have been developed, such as ZRTP [RFC6189],
use OS by design.  This approach for OSRTP is based on [Kaplan06]
where it was called "best effort SRTP".  [Kaplan06] 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 that 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 that 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
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

3.  SDP Offer/Answer Considerations

This section defines the SDP offer/answer considerations for
opportunistic security.

The procedures are for a specific "m=" section describing RTP-based
media.  If an SDP offer or answer contains multiple such "m="
sections, the procedures are applied to each "m=" section
individually.

"Initial OSRTP offer" refers to the offer in which opportunistic
security is offered for an "m=" section for the first time within an
SDP session.

It is important to note that OSRTP makes no changes to 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], that is
the "comprehensive protection" for media mode.

3.1.  Generating the Initial OSRTP Offer

To indicate support for OSRTP in an SDP offer, the offerer uses the
RTP/AVP profile [RFC3551] or the RTP/AVPF profile [RFC4585] but
includes SRTP keying attributes.  OSRTP is not specific to any key
management technique for SRTP, and multiple key management techniques
can be included on the SDP offer.  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.

3.2.  Generating the Answer

To accept OSRTP, an answerer receiving an offer indicating support
for OSRTP generates an SDP answer containing SRTP keying attributes
that 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.

3.3.  Offerer Processing the Answer

If the offerer of OSRTP receives an SDP answer that does not contain
SRTP keying attributes, then the media session proceeds with RTP.  If
the SDP answer contains SRTP keying attributes, then the associated
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.

3.4.  Modifying the Session

   When an offerer generates a subsequent SDP offer, it should do so
   following the principles of [RFC6337], meaning that the decision to
   create the new SDP offer should not be influenced by what was
   previously negotiated.  For example, if a previous OSRTP offer did
   not result in SRTP being established, the offerer may try again and
   generate a new OSRTP offer as specified in Section 3.1.

4.  Security Considerations

   The security considerations of [RFC4568] 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, which is consistent with the
   Opportunistic Security approach described in [RFC7435].  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.

   While OSRTP does not require authentication of the key agreement
   mechanism, it does need to avoid exposing SRTP keys to eavesdroppers,
   since this could enable passive attacks against SRTP.  Section 8.3 of
   [RFC4568] requires that any messages that contain SRTP keys be
   encrypted, and further says that encryption SHOULD provide end-to-end
   confidentiality protection if intermediaries that could inspect the
   SDP message are present.  At the time of this writing, it is
   understood that the requirement in [RFC4568] for end-to-end
   confidentiality protection is commonly ignored.  Therefore, if OSRTP
   is used with SDP Security Descriptions, any such intermediaries
   (e.g., SIP proxies) must be assumed to have access to the SRTP keys.

   As discussed in [RFC7435], OSRTP is used in cases where support for
   encryption by the other party is not known in advance and is 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.  IANA Considerations

   This document has no actions for IANA.

6.  References

6.1.  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>.

   [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,
              <https://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, <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>.

   [RFC8174]  Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2.  Informative References

   [Kaplan06] Kaplan, H. and F. Audet, "Session Description Protocol
              (SDP) Offer/Answer Negotiation For Best-Effort Secure
              Real-Time Transport Protocol", Work in Progress,
              draft-kaplan-mmusic-best-effort-srtp-01, October 2006.

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

   [RFC6337]  Okumura, S., Sawada, T., and P. Kyzivat, "Session
              Initiation Protocol (SIP) Usage of the Offer/Answer
              Model", RFC 6337, DOI 10.17487/RFC6337, August 2011,
              <https://www.rfc-editor.org/info/rfc6337>.

Authors' Addresses

    Alan Johnston
    Villanova University
    Villanova, PA
    United States of America

    Email: alan.b.johnston@gmail.com


    Bernard Aboba
    Microsoft
    One Microsoft Way
    Redmond, WA  98052
    United States of America

    Email: bernard.aboba@gmail.com


    Andrew Hutton
    Atos
    Mid City Place
    London  WC1V 6EA
    United Kingdom

    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