DISPATCH Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 1, 2016

A. Johnston
Unaffiliated
B. Aboba
Microsoft
A. Hutton
Unify
L. Liess
Deutsche Telekom
T. Stach
Unaffiliated
February 29, 2016

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

draft-johnston-dispatch-osrtp-02

Abstract

Opportunistic Secure Real-time Transport Protocol (OSRTP) allows encrypted media to be used in environments where support for encryption is not known in advance, and not required. OSRTP is an implementation of Opportunistic Security, as defined in RFC 7435. OSRTP does not require advanced SDP extensions or features and is fully backwards compatible with existing secure and insecure implementations. 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.

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 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 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 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 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 plans to include support in the SIPconnect 2.0 SIP trunking recommendation [SIPCONNECT] which is under development. 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, <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>.

[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>.

[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>.

[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>.

[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, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc6982>.

[SIPCONNECT]
"SIP-PBX / Service Provider Interoperability SIPconnect 2.0 - DRAFT Technical Recommendation", SIP Forum http://www.sipforum.org/content/view/179/213/, 2015, <http://www.sipforum.org>.

Authors' Addresses

Alan Johnston
Unaffiliated
Bellevue, WA
USA

Email: alan.b.johnston@gmail.com

Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

Email: bernard.aboba@gmail.com

Andy Hutton
Unify
Technology Drive
Nottingham NG9 1LA
UK

Email: andrew.hutton@unify.com

Laura Liess
Deutsche Telekom
Heinrich-Hertz-Strasse 3-7
Darmstadt 64295
Germany

Email: laura.liess.dt@googlemail.com

Thomas Stach
Unaffiliated

Email: thomass.stach@gmail.com

Network Working Group J. Peterson
Internet-Draft Neustar
Intended status: Best Current Practice E. Rescorla
Expires: January 9, 2017 R. Barnes
Mozilla
R. Housley
Vigilsec
July 8, 2016

Best Practices for Securing RTP Media Signaled with SIP
draft-peterson-sipbrandy-rtpsec-00.txt

Abstract

Although the Session Initiation Protocol (SIP) includes a suite of security services that has been expanded by numerous specifications over the years, there is no single place that explains how to use SIP to establish confidential media sessions. Additionally, existing mechanisms have some feature gaps that need to be identified and resolved in order for them to address the pervasive monitoring threat model. This specification describes best practices for negotiating confidential media with SIP, including both comprehensive protection solutions which bind the media to SIP-layer identities as well as opportunistic security solutions.

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] includes a suite of security services, ranging from Digest authentication for authenticating entities with a shared secret, to TLS for transport security, to S/MIME (optional) for body security. SIP is frequently used to establish media sessions, in particular audio or audiovisual sessions, which have their own security mechanisms available, such as Secure RTP [RFC3711]. However, the practices needed to bind security at the media layer to security at the SIP layer, to provide an assurance that protection is in place all the way up the stack, rely on a great many external security mechanisms and practices, and require a central point of documentation to explain their optimal use as a best practice.

Revelations about widespread pervasive monitoring of the Internet have led to a reevaluation of the threat model for Internet communications [RFC7258]. In order to maximize the use of security features, especially of media confidentiality, opportunistic measures must often serve as a stopgap when a full suite of services cannot be negotiated all the way up the stack. This document explains the limitations that may inhibit the use of comprehensive protection, and provides recommendations for which external security mechanisms implementers should use to negotiate secure media with SIP. It moreover gives a gap analysis of the limitations of existing solutions, and specifies solutions to address them.

Various specifications that user agents must implement to support media confidentiality are given in the sections below; a summary of the best current practices appears in Section 8.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] and RFC 6919 [RFC6919].

3. Security at the SIP and SDP layer

There are two approaches to providing confidentiality for media sessions set up with SIP: comprehensive protection and opportunistic security (as defined in [RFC7435]).

3.1. Comprehensive Protection

Comprehensive protection for media sessions established by SIP requires the interaction of three protocols: SIP, the Session Description Protocol (SDP), and the Real-time Protocol, in particular its secure profile SRTP. Broadly, it is the responsibility of SIP to provide integrity for the media keying attributes conveyed by SDP, and those attributes will in turn identify the keys used by endpoints in the RTP media session that SDP negotiates. In that way, once SIP and SDP have exchanged the necessary information to initiate a session, the media endpoints will have a strong assurance that the keys they exchange have not been tampered with by third parties, and that end-to-end confidentiality is available.

Our current target mechanism for establishing the identity of the endpoints of a SIP session is the use of STIR [I-D.ietf-stir-rfc4474bis]. The STIR signature has been designed to prevent a class of impersonation attacks that are commonly used in robocalling, voicemail hacking, and related threats. STIR generates a signature over certain features of SIP requests, including header field values that contain an identity for the originator of the request, such as the From header field or P-Asserted-Identity field, and also over the media keys in SDP if they are present. As currently defined, STIR only provides a signature over the "a=fingerprint" attribute, which is a key fingerprint utilized by DTLS-SRTP [RFC5763]; consequently, STIR only offers comprehensive protection for SIP sessions, in concert with SDP and SRTP, when DTLS-SRTP is the media security service. The underlying security object of STIR is extensible, however, and it would be possible to provide signatures over other SDP attributes that contain alternate keying material. A profile for using STIR to provide media confidentiality is given in Section 4.

3.2. Opportunistic Security

Work is already underway on defining approaches to opportunistic media security for SIP in [I-D.johnston-dispatch-osrtp], which builds on the prior efforts of [I-D.kaplan-mmusic-best-effort-srtp]. The major protocol change proposed by that draft is to signal the use of opportunistic encryption by negotiating the AVP profile in SDP, rather than the SAVP profile (as specified in [RFC3711]) that would ordinarily be used when negotiating SRTP.

Opportunistic encryption approaches typically have no integrity protection for the keying material in SDP. Sending SIP over TLS hop-by-hop between user agents and any intermediaries will reduce the prospect that active attackers can alter keys for session requests on the wire. However, opportunistic confidentiality for media will prevent passive attacks of the form most common in the threat of pervasive monitoring.

4. STIR Profile for Endpoint Authentication and Verification Services

A STIR [I-D.ietf-stir-rfc4474bis] verification service can act in concert with an SRTP media endpoint to ensure that the key fingerprints, as given in SDP, match the keys exchanged to establish DTLS-SRTP. Typically, the verification service function would in this case be implemented in the SIP UAS, which would be composed with the media endpoint. If the STIR authentication service or verification service functions are implemented at an intermediary rather than an endpoint, this introduces the possibility that the intermediary could act as a man-in-the-middle, altering key fingerprints. As this attack is not in STIR’s core threat model, which focuses on impersonation rather than man-in-the-middle attacks, STIR offers no specific protections against it. However, it would be possible to build a deployment profile of STIR for media confidentiality which shifts these responsibilities to the endpoints rather than the intermediaries.

In order to be compliant with best practices for SIP media confidentiality with comprehensive protection, user agent implementations MUST implement both the authentication service and verification service roles described in [I-D.ietf-stir-rfc4474bis].

When generating either an offer or an answer, compliant implementations MUST include an "a=fingerprint" attribute containing the fingerprint of an appropriate key (see Section 4.1).

4.1. Credentials

In order to implement the authentication service function, SIP endpoints must acquire the credentials needed to sign for their own identity. That identity is typically carried in the From header field of a SIP request, and either contains a greenfield SIP URI (e.g. "sip:alice@example.com") or a telephone number, which can appear in a variety of ways (e.g. "sip:+17004561212@example.com). [I-D.ietf-stir-rfc4474bis] Section 7 contains guidance for separating the two, and determining what sort of credential is needed to sign for each.

To date, few commercial certificate authorities issue certificates for SIP URIs or telephone numbers. This is one reason why the STIR standard is architected to permit intermediaries to act as an authentication service on behalf of an entire domain, just as in SIP an proxy server can provide domain-level SIP service. While certificate authorities that offered proof-of-possession certificates similar to those used in the email world could be offered for SIP, either for greenfield identifiers or for telephone numbers, this specification does not require their use.

For users who do not possess such certificates, DTLS-SRTP [RFC5763] permits the use of self-signed keys. This profile of STIR for media confidentiality therefore relaxes the authority requirements of [I-D.ietf-stir-rfc4474bis] to allow the use of self-signed keys for authentication services that are composed with user agents, by generating a certificate (per the guidance of [I-D.ietf-stir-certificates]) with a subject corresponding to the user’s identity. Such a credential could be used for trust on first use (see [RFC7435]) by relying parties. Note that relying parties SHOULD NOT use certificate revocation mechanisms or real-time certificate verification systems for self-signed certificates as they will not increase confidence in the certificate.

Users who wish to remain anonymous can instead generate self-signed certificates as described in Section 4.2.

4.2. Anonymous Communications

In some cases, the identity of the initiator of a SIP session may be withheld due to user or provider policy. Per the recommendations of [RFC3323], this may involve using an identity such as "anonymous@anonymous.invalid" in the identity fields of a SIP request. [I-D.ietf-stir-rfc4474bis] does not currently permit authentication services to sign for requests that supply this identity. It does however permit signing for valid domains, such as "anonymous@example.com," as a way of implementation an anonymization service as specified in [RFC3323].

Even for anonymous sessions, providing media confidentiality and partial SDP integrity is still desirable. This specification RECOMMENDS using one-time self-signed certificates for anonymous communications, with a subjectAltName of "sip:anonymous@anonymous.invalid". After a session is terminated, the certificate should be discarded, and a new one, with new keying material, should be generated before each future anonymous call. As with self-signed certificates, relying parties SHOULD NOT use certificate revocation mechanisms or real-time certificate verification systems for anonymous certificates as they will not increase confidence in the certificate.

4.3. Connected Identity Usage

STIR [I-D.ietf-stir-rfc4474bis] provides integrity protection for the SDP bodies of SIP requests, but not SIP responses. When a session is established, therefore, any SDP body carried by a 200 class response in the backwards direction will not be protected by an authentication service and cannot be verified. Thus, sending a secured SDP body in the backwards direction will require an extra RTT, typically a request sent in the backwards direction.

The problem of providing "Connected Identity" for the original RFC4474 was explored in [RFC4916], which uses a provisional or mid-dialog UPDATE request in the backwards direction to convey an Identity header for the recipient of an INVITE. The procedures in that specification are largely compatible with the revision of the Identity header in [I-D.ietf-stir-rfc4474bis]. However, the following updates to [RFC4916] are required:

> The UPDATE carrying signed SDP with a fingerprint in the backwards direction MUST be sent during dialog establishment, following the receipt of a PRACK after a provisional 1xx response.

For use with this STIR Profile for media confidentiality, the UAS that responds to the INVITE request MUST act as an authentication service for the UPDATE sent in the backwards direction.

The use of RFC4916 has some further interactions with ICE; see Section 7.

5. Media Security Protocols

As there are several ways to negotiate media security with SDP, any of which might be used with either opportunistic or comprehensive protection, further guidance to implementers is needed. In [I-D.johnston-dispatch-osrtp], opportunistic approaches considered include DTLS-SRTP, security descriptions [RFC4568], and ZRTP [RFC6189]. In order to prevent men-in-the-middle from decrypting media traffic, the "a=crypto" SDP parameter of security descriptions requires signaling confidentiality which STIR and related comprehensive protection approaches cannot provide, so delivering keys by value in SDP in this fashion is NOT RECOMMENDED. Both DTLS-SRTP and ZRTP instead provide hashes which are carried in SDP, and thus require only integrity protection rather than confidentiality.

Of DTLS-SRTP and ZRTP, only DTLS-SRTP is a Standards Track Internet protocol. For that reason, this specification REQUIRES support for DTLS-SRTP, and allows support for other media security protocols OPTIONALLY.

[TBD] Future versions of this specification will explore the issue of multiple fingerprints appearing in the message, and offers that include both DTLS-SRTP and ZRTP security.

6. Relayed Media and Conferencing

Providing end-to-end media confidentiality for SIP is complicated by the presence of many forms of media relays. While many media relays merely proxy media to a destination, others present themselves as media endpoints and terminate security associations before re-originating media to its destination.

Centralized conference bridges are one type of entity that typically terminates a media session in order to mux media from multiple sources and then to re-originate the muxed media to conference participants. In many such implementations, only hop-by-hop media confidentiality is possible. Work is ongoing to specify a means to encrypt both the hop-by-hop media between a user agent and a centralized server as well as the end-to-end media between user agents. As this is the best practice for supporting [I-D.ietf-perc-double].

Another class of entities that might relay SIP media are back-to-back user agents (B2BUAs). If a B2BUA follows the guidance in [RFC7879], it may be possible for those devices to act as media relays while still permitting end-to-end confidentiality between user agents.

Ultimately, if an endpoint can decrypt media it receives, then that endpoint can forward the decrypted media without the knowledge or consent of the media's originator. No media confidentiality mechanism can protect against these sorts of relayed disclosures, or trusted entities that can decrypt media and then record a copy to be sent elsewhere (see [RFC7245]).

7. ICE and Connected Identity

Providing confidentiality for media with comprehensive protection requires careful timing of when media streams should be sent and when a user interface should signify that confidentiality is in place.

In order to best enable end-to-end connectivity between user agents, and to avoid media relays as much as possible, implementations of this specification must support ICE [I-D.ietf-ice-rfc5245bis]. To speed up call establishment, it is RECOMMENDED that implementations support trickle ICE [I-D.ietf-mmusic-trickle-ice-sip].

Note that in the comprehensive protection case, the use of Connected Identity [RFC4916] with ICE entails that the answer containing the key fingerprints, and thus the STIR signature, will come in an UPDATE sent in the backwards direction a provisional response and acknowledgment (PRACK), rather than in any earlier SDP body. Only at such a time as that UPDATE is received will the media keys be considered exchanged in this case.

Similarly, in order to prevent, or at least mitigate, the denial-of-service attack envisioned in [RFC5245] Section 18.5.1, this specification incorporates best practices for ensuring that recipients of media flows have consented to receive such flows. Implementations of this specification MUST implement the STUN usage for consent freshness defined in [RFC7675].

8. Best Current Practices

The following are the best practices for SIP user agents to provide media confidentiality for SIP sessions.

Implementations MUST support the STIR endpoint profile given in Section 4.

Implementations MUST support DTLS-SRTP for key-management, as described in Section 5.

Implementations MUST support the ICE, and the STUN consent freshness mechanism, as specified in Section 7.

Implementations MUST support the PERC "double" mechanism, as specifies in Section 6.

9. Acknowledgments

We would like to thank Adam Roach, Andrew Hutton, and Ben Campbell for contributions to this problem statement and framework.

10. IANA Considerations

This memo includes no requests to the IANA.

11. Security Considerations

This document describes the security features that provide media sessions established with SIP with confidentiality, integrity, and authentication.

12. Informative References

[I-D.ietf-ice-rfc5245bis]
Keranen, A., Holmberg, C., and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal", draft-ietf-ice-rfc5245bis-04 (work in progress), June 2016.

[I-D.ietf-mmusic-trickle-ice-sip]
Ivov, E., Stach, T., Marocco, E., and C. Holmberg, "A Session Initiation Protocol (SIP) usage for Trickle ICE", draft-ietf-mmusic-trickle-ice-sip-04 (work in progress), May 2016.

[I-D.ietf-perc-double]
Jennings, C., Jones, P., and A. Roach, "SRTP Double Encryption Procedures", draft-ietf-perc-double-01 (work in progress), July 2016.

[I-D.ietf-stir-certificates]
Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-06 (work in progress), July 2016.

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-09 (work in progress), May 2016.

[I-D.johnston-dispatch-osrtp]
Johnston, A., Ph.D., D., Hutton, A., Liess, L., and T. Stach, "An Opportunistic Approach for Secure Real-time Transport Protocol (OSRTP)", draft-johnston-dispatch-osrtp-02 (work in progress), February 2016.

[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.

[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>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[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>.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, DOI 10.17487/RFC3323, November 2002, <http://www.rfc-editor.org/info/rfc3323>.

[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>.

[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>.

[RFC4916] Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, DOI 10.17487/RFC4916, June 2007, <http://www.rfc-editor.org/info/rfc4916>.

[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>.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, DOI 10.17487/RFC5245, April 2010, <http://www.rfc-editor.org/info/rfc5245>.

[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, <http://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, <http://www.rfc-editor.org/info/rfc6189>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, DOI 10.17487/RFC6919, April 2013, <http://www.rfc-editor.org/info/rfc6919>.

[RFC7245] Hutton, A., Ed., Portman, L., Ed., Jain, R., and K. Rehor, "An Architecture for Media Recording Using the Session Initiation Protocol", RFC 7245, DOI 10.17487/RFC7245, May 2014, <http://www.rfc-editor.org/info/rfc7245>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[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>.

[RFC7675] Perumal, M., Wing, D., Ravindranath, R., Reddy, T., and M. Thomson, "Session Traversal Utilities for NAT (STUN) Usage for Consent Freshness", RFC 7675, DOI 10.17487/RFC7675, October 2015, <http://www.rfc-editor.org/info/rfc7675>.

[RFC7879] Ravindranath, R., Reddy, T., Salgueiro, G., Pascual, V., and P. Ravindran, "DTLS-SRTP Handling in SIP Back-to-Back User Agents", RFC 7879, DOI 10.17487/RFC7879, May 2016, <http://www.rfc-editor.org/info/rfc7879>.

Authors' Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Eric Rescorla
Mozilla

Email: ekr@rtfm.com

Richard Barnes
Mozilla

Email: rbarnes@mozilla.com

Russ Housley
Vigilsec

Email: rhousley@vigilsec.com