Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: October 27, 2019

J. Peterson
Neustar
R. Barnes
Cisco
R. Housley
Vigil Security
April 25, 2019

Best Practices for Securing RTP Media Signaled with SIP
draft-ietf-sipbrandy-rtpsec-08

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 a comprehensive protection solution that binds the media layer to SIP layer identities.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 27, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261] includes a suite of security services, including Digest authentication, for authenticating entities with a shared secret, TLS for transport security, and S/MIME (optionally) 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. This document provides documentation to explain their optimal use as a best practice.

Revelations about widespread pervasive monitoring of the Internet have led to a greater desire to protect Internet communications

[RFC7258]. In order to maximize the use of security features, especially of media confidentiality, opportunistic measures serve as a stopgap when a full suite of services cannot be negotiated all the way up the stack. Opportunistic media security for SIP is described in [I-D.ietf-sipbrandy-osrtp], which builds on the prior efforts of [I-D.kaplan-mmusic-best-effort-srtp]. With opportunistic encryption, there is an attempt to negotiate the use of encryption, but if the negotiation fails, then cleartext is used. Opportunistic encryption approaches typically have no integrity protection for the keying material.

This document contains the SIPBRANDY profile of STIR [RFC8224] for media confidentiality, providing a comprehensive security solution for SIP media that includes integrity protection for keying material and offers application-layer assurance that media confidentiality is place. 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

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. 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]). This document only addresses comprehensive protection.

Comprehensive protection for media sessions established by SIP requires the interaction of three protocols: Session Initiation Protocol (SIP) [RFC3261], the Session Description Protocol (SDP) [RFC4566], and the Real-time Protocol (RTP) [RFC3550], in particular its secure profile Secure RTP (SRTP) [RFC3711]. Broadly, it is the responsibility of SIP to provide integrity protection 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(s) that SDP negotiates.

Note that this framework does not apply to keys that also require confidentiality protection in the signaling layer, such as the SDP "k=" line, which MUST NOT be used in conjunction with this profile.

In that way, once SIP and SDP have exchanged the necessary information to initiate a session, 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.

To establishing the identity of the endpoints of a SIP session, this specification uses STIR [RFC8224]. The STIR Identity header 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 provides a signature over the "a=fingerprint" attribute, which is a fingerprint of the key used 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 PASSporT [RFC8225] object used by 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.

4. STIR Profile for Endpoint Authentication and Verification Services

STIR [RFC8224] defines the Identity header field for SIP, which provides a cryptographic attestation of the source of communications. This document includes a profile of STIR, called the SIPBRANDY profile, where the STIR verification service will 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. To satisfy this condition, the verification service function would in this case be implemented in the SIP User Agent Server (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 such interference.

The SIPBRANDY profile for media confidentiality thus shifts these responsibilities to the endpoints rather than the intermediaries. While intermediaries MAY provide the verification service function of STIR for SIPBRANDY transactions, the verification needs to be repeated at the endpoint to obtain end-to-end assurance. Intermediaries supporting this specification MUST NOT block or otherwise redirect calls if they do not trust the signing credential.

The SIPBRANDY profile is based on an end-to-end trust model, so it is up to the endpoints to determine if they support signing credentials, not 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 [RFC8224]. STIR authentication services MUST signal their compliance with this specification by including the "msec" claim defined in this specification to the PASSporT payload. Implementations MUST provide key fingerprints in SDP and the appropriate signatures over them as specified in [RFC8225].

When generating either an offer or an answer [RFC3264], 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 in the user agent, SIP endpoints will need to 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;user=phone"). Section 8 of [RFC8224] contains guidance for separating the two, and determining what sort of credential is needed to sign for each.

To date, few commercial certification authorities (CAs) issue certificates for SIP URIs or telephone numbers; though work is ongoing on systems for this purpose (such as [I-D.ietf-acme-authority-token]) it is not yet mature enough to be recommended as a best practice. This is one reason why STIR permits intermediaries to act as an authentication service on behalf of an entire domain, just as in SIP a proxy server can provide domain-level SIP service. While CAs that offer proof-of-possession certificates similar to those used for email 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 public keys. This profile of STIR employs more relaxed authority requirements of [RFC8224] to allow the use of self-signed public keys for authentication services that are composed with user agents, by generating a certificate (per the guidance in [RFC8226]) with a subject corresponding to the user's

identity. To obtain comprehensive protection with a self-signed certificate, some out-of-band verification is needed as well. 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.

Generally speaking, without access to out-of-band information about which certificates were issued to whom, it will be very difficult for relying parties to ascertain whether or not the signer of a SIP request is genuinely an "endpoint." Even the term "endpoint" is a problematic one, as SIP user agents can be composed in a variety of architectures and may not be devices under direct user control. While it is possible that techniques based on certificate transparency [RFC6962] or similar practices could help user agents to recognize one another's certificates, those operational systems will need to ramp up with the CAs that issue credentials to end user devices going forward.

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. Following the recommendations of [RFC3323], this may involve using an identity such as "anonymous@anonymous.invalid" in the identity fields of a SIP request. [RFC8224] 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 fresh 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.

Note that when using one-time anonymous self-signed certificates, any man in the middle could strip the Identity header and replace it with one signed by its own one-time certificate, changing the "mkey" parameters of PASSporT and any "a=fingerprint" attributes in SDP as it chooses. This signature only provides protection against non-Identity aware entities that might modify SDP without altering the PASSporT conveyed in the Identity header.

4.3. Connected Identity Usage

STIR [RFC8224] provides integrity protection for the fingerprint attributes in SIP request bodies, 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" in [RFC4474], which is obsoleted by STIR, was explored in [RFC4916], which uses a provisional or mid-dialog UPDATE request in the backwards direction to convey an Identity header field for the recipient of an INVITE. The procedures in that specification are largely compatible with the revision of the Identity header in STIR [RFC8224]. However, the following need to be considered:

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

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

The text in Section 4.4.1 of [RFC4916] regarding the receipt at a UAC of error codes 428, 436, 437 and 438 in response to a mid-dialog request RECOMMENDS treating the dialog as terminated. However, Section 6.1.1 of [RFC8224] allows the retransmission of requests with repairable error conditions. In particular, an authentication service might retry a mid-dialog rather than treating the dialog as terminated, although only one such retry is permitted.

Note that the examples in [RFC4916] are based on the original [RFC4474], and will not match signatures using STIR [RFC8224].

Future work may be done to revise [RFC4916] for STIR; that work should take into account any impacts on the SIPBRANDY profile described in this document. The use of [RFC4916] has some further interactions with ICE; see Section 7.

4.4. Authorization Decisions

[RFC8224] grants STIR verification services a great deal of latitude when making authorization decisions based on the presence of the Identity header field. It is largely a matter of local policy whether an endpoint rejects a call based on absence of an Identity header field, or even the presence of a header that fails an integrity check against the request.

For this SIPBRANDY profile of STIR, however, a compliant verification service that receives a dialog-forming SIP request containing an Identity header with a PASSporT type of "msec", after validating the request per the steps described in Section 6.2 of [RFC8224], MUST reject the request if there is any failure in that validation process with the appropriate status code per Section 6.2.2. If the request is valid, then if a terminating user accepts the request, it MUST then follow the steps in Section 4.3 to act as an authentication service and send a signed request with the "msec" PASSPorT type in its Identity header as well, in order to enable end-to-end bidirectional confidentiality.

For the purposes of this profile, the "msec" PASSporT type can be used by authentication services in one of two ways: as a mandatory request for media security, or as a merely opportunistic request for media security. As any verification service that receives an Identity header field in a SIP request with an unrecognized PASSporT type will simply ignore that Identity header, an authentication service will know whether or not the terminating side supports "msec" based on whether or not its user agent receives a signed request in the backwards direction per Section 4.3. If no such requests are received, the UA may do one or two things: shut down the dialog, if the policy of the UA requires that "msec" be supported by the terminating side for this dialog; or, if policy permits (e.g., an explicit acceptance by the user), allow the dialog to continue without media security.

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.ietf-sipbrandy-osrtp], opportunistic approaches considered

include DTLS-SRTP, security descriptions [RFC4568], and ZRTP [RFC6189].

Support for DTLS-SRTP is REQUIRED by this specification.

The "mkey" claim of PASSporT provides integrity protection for "a=fingerprint" attributes in SDP, including cases where multiple "a=fingerprint" attributes appear in the same SDP.

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, but is not sufficiently mature at this time to make a recommendation for a best practice here. Those protocols are expected to identify their own best practice recommendations as they mature.

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 [RFC8445]. 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 a provisional 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 described in Section 19.5.1 of [RFC8445], 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, and signal that in PASSporT with the "msec" header element.

Implementations MUST follow the authorization decision behavior in Section 4.4.

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.

9. IANA Considerations

This specification defines a new value for the Personal Assertion Token (PASSporT) Extensions registry called "msec," and the IANA is requested to add that entry to the registry with a value pointing to [RFCThis].

10. Security Considerations

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

11. Acknowledgments

We thank Eric Rescorla, Adam Roach, Andrew Hutton, and Ben Campbell for contributions to this problem statement and framework. We thank Liang Xia and Alissa Cooper for their careful review.

12. References

12.1. Normative References

[I-D.ietf-mmusic-trickle-ice-sip] Ivov, E., Stach, T., Marocco, E., and C. Holmberg, "A Session Initiation Protocol (SIP) Usage for Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (Trickle ICE)", draft-ietf-mmusic-trickle-ice-sip-18 (work in progress), June 2018.

[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>.

[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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc3323>.

[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>.

[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>.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, DOI 10.17487/RFC4566, July 2006, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc4916>.

[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>.

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

[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, <https://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, <https://www.rfc-editor.org/info/rfc7879>.

[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>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/info/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

[RFC8445] Keranen, A., Holmberg, C., and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal", RFC 8445, DOI 10.17487/RFC8445, July 2018, <https://www.rfc-editor.org/info/rfc8445>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

12.2. Informative References

[I-D.ietf-acme-authority-token]
Peterson, J., Barnes, M., Hancock, D., and C. Wendt, "ACME Challenges Using an Authority Token", draft-ietf-acme-authority-token-03 (work in progress), March 2019.

[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-08 (work in progress), March 2019.

[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.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, DOI 10.17487/RFC4474, August 2006, <https://www.rfc-editor.org/info/rfc4474>.

[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>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/info/rfc6962>.

[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, <https://www.rfc-editor.org/info/rfc7245>.

[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>.

Authors' Addresses

Jon Peterson
Neustar, Inc.

Email: jon.peterson@team.neustar

Richard Barnes
Cisco

Email: rlb@ipv.sx

Russ Housley
Vigil Security, LLC

Email: housley@vigilsec.com

Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: January 9, 2017

J. Peterson
Neustar
E. Rescorla
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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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