Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 26, 2021

J. Peterson
Neustar
C. Wendt
Comcast

February 22, 2021

Messaging Use Cases and Extensions for STIR
draft-peterson-stir-messaging-01

Abstract

Secure Telephone Identity Revisited (STIR) provides a means of attesting the identity of a telephone caller via a signed token in order to prevent impersonation of a calling party number, which is a key enabler for illegal robocalling. Similar impersonation is sometimes leveraged by bad actors in the text messaging space. This document considers the applicability of STIR's Persona Assertion Token (PASSporT) and certificate issuance framework to instant text and multimedia messaging use cases, both for messages carried or negotiated by SIP, and for non-SIP messaging.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The STIR problem statement [RFC7340] describes widespread problems enabled by impersonation in the telephone network, including illegal robocalling, voicemail hacking, and swatting. As telephone services are increasingly migrating onto the Internet and using Voice over IP (VoIP) protocols such as SIP [RFC3261], it is necessary for these protocols to support stronger identity mechanisms to prevent impersonation. [RFC8224] defines a SIP Identity header field capable of carrying PASSporT [RFC8225] objects in SIP as a means to cryptographically attest that the originator of a telephone call is authorized to use the calling party number (or, for native SIP cases, SIP URI) associated with the originator of the call.

The problem of bulk, unsolicited commercial communications is not however limited to telephone calls. Although the problem is not currently widespread, in some environments spammers and fraudsters are turning to messaging applications to deliver undesired content to consumers. In some respects, mitigating these unwanted messages resembles the email spam problem: textual analysis of the message contents can be used to fingerprint content that is generated by spammers, for example. However, encrypted messaging is becoming more common, and analysis of message contents may no longer be a reliably

way to mitigate messaging spam in the future. And as STIR sees further deployment in the telephone network, it seems likely that the governance structures put in place for securing telephone network resources with STIR could be repurposed to help secure the messaging ecosystem.

One of the more sensitive applications for message security is emergency services. As next-generation emergency services increasingly incorporate messaging as a mode of communication with public safety personnel (see [RFC8876]), providing an identity assurance could help to mitigate denial-of-service attacks, as well as ultimately helping to identify the source of emergency communications in general (including the swatting attacks, see [RFC7340]).

This specification therefore explores how the PASSporT mechanism defined for STIR could be applied to providing protection for textual and multimedia messaging, but focuses particularly on those messages that use telephone numbers as the identity of the sender. It moreover considers the reuse of existing STIR certificates, which are beginning to see widespread deployment, for signing PASSporTs that protect messages.

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. Applicability to Messaging Systems

At a high level, baseline PASSporT [RFC8225] claims provide similar value to number-based messaging as they do to traditional telephone calls. A signature over the calling and called party numbers, along with a timestamp, could already help to prevent impersonation in the mobile messaging ecosystem. When it comes to protecting message contents, broadly, there are a few ways that the PASSporT mechanism of STIR could apply to messaging: first, a PASSporT could be used to securely negotiate a session over which messages will be exchanged; and second, in sessionless scenarios, a PASSporT could be generated on a per-message basis with its own built-in message security.

3.1. Message Sessions

For the first case, where SIP negotiates a session where the media will be text messages, as for example with the Message Session Relay Protocol (MSRP) [RFC4975], the usage of STIR would deviate little from [RFC8224]. An INVITE request sent with an Identity header containing a PASSporT with the proper calling and called party numbers would then negotiate an MSRP session the same way that an INVITE for a telephone call would negotiate an audio session. This could be applicable to MSRP sessions negotiated for RCS [RCC.07]. Note that if TLS is used to secure MSRP (per RCS [RCC.15]), fingerprints of those TLS keys could be secured via the "mkey" claim of PASSporT using the [RFC8862] framework. Similar practices would apply to sessions that negotiate text over RTP via [RFC4103] or similar mechanisms. For the most basic use cases, STIR for messaging should not require any further protocol enhancements.

[TBD: liase with GSMA on this]

However, current usage of baseline [RFC8224] Identity is largely confined to INVITE requests. RCS-style applications would require PASSporTs for all conversation participants. This would in turn require the implementation of STIR connected identity [I-D.peterson-stir-rfc4916-update].

3.2. PASSporTs and Messaging

In the second case, SIP also has a method for sending messages in the body of a SIP request: the MESSAGE [RFC3428] method, which is used in some North American emergency services use cases. The interaction of STIR with MESSAGE is not as straightforward as the potential use case with MSRP. An Identity header could be added to any SIP MESSAGE request, but without some extension to the PASSporT claims, the PASSporT would offer no protection to the message content. As the bodies of SIP requests are MIME encoded, S/MIME [RFC8591] has been proposed as a means of providing integrating for MESSAGE (and some MSRP cases as well). The interaction of [RFC8226] STIR certificates with S/MIME for messaging applications would require some further explication; and potentially, PASSporT could provide its own integrity check for message contents.

Moreover, a variety of non-SIP protocols, both those integrated into the traditional telephone network and those based on over-the-top applications, are responsible for most of the messaging that is sent to and from telephone numbers. This specification proposes that the STIR credentials assigned to service providers could be leveraged to sign for PASSporTs for messages that originate from telephone numbers. In order to apply PASSporT to textual or multimedia

messaging, a new claim is here defined to provide a hash over message contents.

In order to differentiate a PASSporT for an individual message from a PASSporT used to secure a telephone call or message stream, this document defines a new "msg" PASSporT Type. This helps to prevent the replay of a PASSporT for a message to putatively secure a call, or vice versa.

This specification defines a new optional JWT [RFC7519] claim "msgi" which provides a digest over the contents of a message, which may be a text message, or a more complex multimedia message. "msgi" MUST NOT appear in PASSporTs with a type other than "msg", but they are OPTIONAL in "msg" PASSporTs, as integrity for messages may be provided by some other service (e.g. [RFC8591]). Implementations of "msgi" MUST support the following hash algorithms: "SHA256", "SHA384", or "SHA512", which are defined as part of the SHA-2 set of cryptographic hash functions by the NIST.

[TBD: Do we need algorithmic agility here?]

In order to generate the message digest, the following steps are taken:

[TBD: Canonicalization procedures. Maybe we need separate procedures for plain text (like, SMPP), rich text, and then more complex multimedia messages? Definitely a danger of scope creep. For the emergency services case, we want OASIS CAP, right? Maybe focus on that. Anything we could easily steal here?]

At the end result of the process, the digest becomes the value of the JWT "msgi" claim, as per this example:

```
"msgi" :
"sha256-H8BRh8j48O9oYatfu5AZzq6A9RINQZngK7T62em8MUt1FLm52t+eX6xO"
```

3.2.1. PASSporT Conveyance with Messaging

If the message is being conveyed in SIP, via the MESSAGE method, then the PASSporT could be conveyed in an Identity header field in that request. The authentication and verification service procedures for populating that PASSporT would follow [RFC8224], with the addition of the "msgi" claim defined in Section 3.2.

In text messaging today, multimedia message system (MMS) messages are often conveyed with SMTP. There are thus a suite of additional email security tools available in this environment for sender authentication, such as DMARC [RFC7489]. The interaction of these

mechanisms with STIR certificates and/or PASSporTs would require further study.

For other cases where messages are conveyed by some protocol other than SIP, that protocol might itself have some way of conveying PASSporTs. But there will surely be cases where legacy transmission of messages will not permit an accompanying PASSporT, in which case something like out-of-band [I-D.ietf-stir-oob] conveyance would be the only way to deliver the PASSporT. This may be necessary to support cases where legacy SMPP systems cannot be upgraded, for example.

[TBD: I mean, if you can deliver a PASSporT OOB, you can deliver a message OTT - there may be limits to how useful a mechanism like this would be. In any event, the precise way to do OOB for messaging would need to be sketched out here.]

4. Certificates and Messaging

The [RFC8226] STIR certificate profiles defines a way to issue certificates that sign PASSporTs, which attest through their TNAuthList either a Service Provider Code (SPC), or a set of one or more telephone numbers. This specification proposes that the semantics of this certificates should suffice for signing for messages from a telephone number without further modification.

[TBD: Or should there be? Should for example certificates have to have some special authority to sign for messages instead of calls?]

5. Acknowledgments

We would like to thank Brian Rosen, Ben Campbell, and Alex Bobotek for their contributions to this specification.

6. IANA Considerations

6.1. JSON Web Token Claims Registration

This specification requests that the IANA add one new claim to the JSON Web Token Claims registry as defined in [RFC7519].

Claim Name: "msgi"

Claim Description: Message Integrity Information

Change Controller: IESG

Specification Document(s): [RFCThis]

6.2. PASSporT Type Registration

This specification defines one new PASSporT type for the PASSport Extensions Registry defined in [RFC8225], which resides at https://www.iana.org/assignments/passport/passport.xhtml#passport-extensions. It is:

"msg" as defined in [RFCThis] Section 3.2.

7. Security Considerations

TBD.

8. References

8.1. 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>.

[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>.

[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>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <https://www.rfc-editor.org/info/rfc7159>.

[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>.

8.2. Informative References

[I-D.ietf-stir-oob] Rescorla, E. and J. Peterson, "STIR Out-of-Band Architecture and Use Cases", draft-ietf-stir-oob-07 (work in progress), March 2020.

[I-D.ietf-stir-passport-divert] Peterson, J., "PASSporT Extension for Diverted Calls", draft-ietf-stir-passport-divert-09 (work in progress), July 2020.

[I-D.peterson-stir-rfc4916-update] Peterson, J. and C. Wendt, "Connected Identity for STIR", draft-peterson-stir-rfc4916-update-02 (work in progress), November 2020.

[RCC.07] GSMA RCC.07 v9.0 | 16 May 2018, "Rich Communication Suite 8.0 Advanced Communications Services and Client Specification", 2018.

[RCC.15] GSMA PRD-RCC.15 v5.0 | 16 May 2018, "IMS Device Configuration and Supporting Services", 2018.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, DOI 10.17487/RFC3311, October 2002, <https://www.rfc-editor.org/info/rfc3311>.

[RFC3428] Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, DOI 10.17487/RFC3428, December 2002, <https://www.rfc-editor.org/info/rfc3428>.

[RFC4103] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", RFC 4103, DOI 10.17487/RFC4103, June 2005, <https://www.rfc-editor.org/info/rfc4103>.

[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>.

[RFC4975] Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., "The Message Session Relay Protocol (MSRP)", RFC 4975, DOI 10.17487/RFC4975, September 2007, <https://www.rfc-editor.org/info/rfc4975>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8591] Campbell, B. and R. Housley, "SIP-Based Messaging with S/MIME", RFC 8591, DOI 10.17487/RFC8591, April 2019, <https://www.rfc-editor.org/info/rfc8591>.

[RFC8862] Peterson, J., Barnes, R., and R. Housley, "Best Practices for Securing RTP Media Signaled with SIP", BCP 228, RFC 8862, DOI 10.17487/RFC8862, January 2021, <https://www.rfc-editor.org/info/rfc8862>.

[RFC8876] Rosen, B., Schulzrinne, H., Tschofenig, H., and R. Gellens, "Non-interactive Emergency Calls", RFC 8876, DOI 10.17487/RFC8876, September 2020, <https://www.rfc-editor.org/info/rfc8876>.

Authors' Addresses

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

Email: jon.peterson@team.neustar

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net