Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

J. Peterson
Neustar

November 2, 2020

Out-of-Band STIR for Service Providers
draft-ietf-stir-servprovider-oob-00

Abstract

The Secure Telephone Identity Revisited (STIR) framework defines means of carrying its Persona Assertion Tokens (PASSporTs) either in-band, within the headers of a SIP request, or out-of-band, through a service that stores PASSporTs for retrieval by relying parties. This specification defines a way that the out-of-band conveyance of PASSporTs can be used to support large service providers, for cases in which in-band STIR conveyance is not universally available.

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 May 6, 2021.

Table of Contents

1. Introduction

STIR [RFC8224] provides a cryptographic assurance of the identity of calling parties in order to prevent impersonation, which is a key enabler of unwanted robocalls, swatting, vishing, voicemail hacking, and similar attacks (see [RFC7340]). The STIR out-of-band [I-D.ietf-stir-oob] framework enables the delivery of PASSporT [RFC8225] objects through a Call Placement Service (CPS), rather than carrying them within a signaling protocol such as SIP. Out-of-band conveyance is valuable when end-to-end SIP delivery of calls is partly or entirely unavailable due to network border policies, calls routinely transitting a gateway to the PSTN, or similar circumstances.

While out-of-band STIR can be implemented as an open Internet service, it then requires complex security measures to enable the CPS function without allowing the CPS to collect data about the parties placing calls. This specification describes CPS implementations that act specifically on behalf of service providers who will be processing the calls that STIR secures, and who thus will learn about the parties to communication independently, so an alternative security architecture becomes possible.

Environments that might support this flavor of STIR out-of-band include carriers, large enterprises, call centers, or any Internet service that aggregates on behalf of a large number of telephone endpoints.

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. Service Provider Deployment Architecture for Out-of-Band STIR

The architecture in this specification assumes that every participating service provider will advertise one or more designated CPS instances. A service provider's CPS serves as a place where callers can deposit a PASSporT when attempting to place a call to a subscriber of the destination service provider; if the caller's domain supports in-band STIR, this can be done at the same time as an in-band STIR call is placed. The terminating service provider could operate the CPS themselves, or a third party could operate the CPS on the destination's behalf. This model does not assume a monolithic CPS that acts on behalf of all service providers, but nor does it prohibit multiple service providers from sharing a CPS provider. Moreover, a particular CPS can be a logically distributed entity compromised of several geographically distant entities that flood PASSporTs among themselves to support an anycast-like service.

The process of locating a destination CPS and submitting a PASSporT requires Internet connectivity between the call originator and the CPS. If the CPS is deployed in the terminating service provider network, that network connectivity could be leveraged to initiate a SIP session, during which in-band STIR could be used. The applicability of this architecture is therefore to those cases where, for whatever reason, SIP calls cannot reliably be placed end-to-end, but an HTTP transaction can reliably be sent to the destination network from the out-of-band authentication service (OOB-AS) in the caller's network. It is hoped that as IP connectivity between telephone providers increases, there will be less need for an out-of-band mechanism, but it can serve as a fallback mechanism in cases where service providers cannot predict whether end-to-end delivery of SIP calls will occur.

4. Advertising a CPS

If more than one CPS exists for a given deployment, there will need to be some means of discovering CPSs, either administratively or programmatically. Many services providers have bilateral agreements to peer with one another, and in those environments, identifying their respective CPS's could be a simple matter of provisioning. A consortium of service providers could simply agree to choose from a

list of available CPS providers, say. In more pluralist environments, some mechanism is needed to discover the CPS associated with the target of a call.

In order to allow the CPS chosen by a service provider to be discovered securely, this specification defines a CPS advertisement. Effectively, a CPS advertisement is a document which contains the URL of a CPS, as well as any information needed to determine which PASSporTs should be submitted to that CPS. An advertisement may be signed with a STIR [RFC8226] credential, or another credential that is trusted by the participants in a given STIR environment. The advantage to signing with STIR certificates is that they contain a "TNAuthList" value indicating the telephone network resources that a service provider controls. This information can be matched with a TNAuthList value in the CPS advertisement to determine whether the signer has the authority to advertise a particular CPS as the proper destination for PASSporTs.

The format of a service provider CPS advertisement is a simple JSON object containing one or more pairs of TNAuthList values pointing to the URIs of CPSs, e.g. { "1234":"https://cps.example.com" }. TNAuthList values can be either Service Provider Codes (SPCs) or telephone numbers or number ranges. CPS URIs MUST be HTTPS URIs. [More TBD].

CPS advertisements could be made available through existing or new databases, potentially aggregated across multiple service providers and distributed to call originators as necessary. They could be discovered during the call routing process, including through a DNS lookup. They could be shared through a distributed database among the participants in a multilateral peering arrangement.

An alternative to CPS advertisements that may be usable in some environments is adding a field to STIR [RFC8226] credentials issued to individual service providers. As these certificates are themselves signed by a CA, the URI would be bound securely to the service provider. As STIR assumes a community of relying parties who trust these credentials, this method perhaps best mirrors the trust model required to allow a CPS to authorize PASSporT submission and retrieval.

5. Submitting a PASSporT

Submitting a PASSporT to a CPS as specified in the STIR out-of-band framework [I-D.ietf-stir-oob] requires security measures which are intended to prevent the CPS from learning the identity of the caller (or callee), to the degree possible. In this service provider case, however, the CPS is operated by the service provider of the callee

(or an entity operating on their behalf), and as such the information that appears in the PASSporT is redundant with call signaling that the terminating party will receive anyway. Therefore, the service provider out-of-band framework does not attempt to conceal the identity of the originating or terminating party from the CPS.

An out-of-band authentication service (OOB-AS) forms a secure connection with the target CPS. This may happen at the time a call is being placed, or it may be a persistent connection, if there is a significant volume of traffic sent over this interface. The OOB-AS SHOULD authenticate itself to the CPS using its STIR credential [RFC8226]the same one it would use to sign calls via mutual TLS; this helps mitigate the risk of flooding that more open OOB implementations may face. Furthermore, use of mutual TLS prevents attackers from replaying captured PASSporTs to the CPS. A CPS makes its own policy decision as to whether it will accept calls from a particular OOB-AS, and at what volumes.

Service provider out-of-band PASSporTs do not need to be encrypted for storage at the CPS, although use of transport-layer security to prevent eavesdropping on the connection between the CPS and OOB-ASs is REQUIRED. PASSporTs will be submitted to the CPS at the time they are created by an AS; if the PASSporT is also being used for in-band transit within a SIP request, the PASSporT can be submitted to the CPS before or after the SIP request is sent, at the discretion of the originating domain. An OOB-AS will use a REST interface to submit PASSporTs to the CPS as described in [I-D.ietf-stir-oob] Section 9 [more TBD]. PASSporTs are persisted by the CPS for as long as is required for them to be retrieved (see the next section), but in any event for no longer than the freshness interval of the PASSporT itself (a maximum of sixty seconds).

6. PASSporT Retrieval

The STIR out-of-band framework [I-D.ietf-stir-oob] proposes two means that called parties can acquire PASSporTs out-of-band: through a retrieval interface, or through a subscription interface. In the service provider context, where many calls occur simultaneously, an out-of-band capable verification service may therefore operate in one of two modes: it can either pull PASSporTs from the CPS after calls arrive, or receive push notifications from the CPS for incoming calls.

If a CPS serves only one service provider, then all PASSporTs submitted to the CPS are made available to the OOB-VS of that provider; indeed, the CPS and OOB-VS may be colocated or effectively operated as a consolidated system. In a multi-provider environment, the STIR credential of the terminating domain can be used by the CPS

to determine the range of TNAuthLists for which an OOB-VS is entitled to receive PASSporTs; this may be through a mechanism like mutual TLS, or through using the STIR credential to sign a token that is submitted to the CPS by the retrieving OOB-VS. Note that a CPS will need to inspect the "dest" element of a PASSporT to determine which OOB-VS should receive the PASSporT in this case. [TBD: Which sub/not protocol to use for the case where the CPS and OOB-VS are not composed in a single function?]

Pulling of PASSporTs from the CPS will follow the basic REST flow described in [I-D.ietf-stir-oob] Section 9. In the push interface case, exactly how a CPS determines which PASSporTs to send to an out-of-band verification service is a matter of implementation. An OOB-VS could for example subscribe to a range of telephone numbers, which will be directed to that OOB-VS by the CPS (provided the OOB-VS is authorized to receive them by the CPS).

In the pull model, a terminating service provider contacts the CPS via its OOB-VS after having received a call in cases when the call signaling does not itself carry a STIR signature. In the push model, a PASSporT might be sent to the OOB-VS either before or after unsigned call signaling has been received by the terminating domain. Domains using the push model may therefore need to adopt a model where call signaling is held momentarily in order to await the potential arrival of a PASSporT at the OOB-VS. The exact timing of this, and its interaction with the substitution attack described in [I-D.ietf-stir-oob] Section 7.4, will be the covered by future versions of this specification.

7. Gateways

In some deployment architectures, gateways might perform a function that interfaces with a CPS for the retrieval or storage of PASSporTs. For example, a closed network of in-band STIR providers may send SIP INVITEs to a gateway in front of a traditional PSTN tandem that services a set of legacy service providers. In that environment, a gateway might take a PASSporT out of in-band SIP INVITEs and store it in a CPS that was established to handle requests for one or more legacy providers, who in turn consume those PASSporTs through an OOB-VS to assist in robocall mitigation and similar functions.

The simplest way to interface a gateway performing this sort of function for a service provider CPS system is to issue credentials to the gateway that allow it to act on behalf of the legacy service providers it supports: this would allow it to both add PASSporTs to the CPS acting on behalf of the legacy providers, and also to create PASSporTs for in-band STIR conveyance from the legacy-providers to terminating service providers in the closed STIR network.

8. Acknowledgments

We would like to thank Alex Fenichel for contributions to this specification.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

TBD.

11. 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.

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

Author's Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@neustar.biz