

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

J. Peterson
Neustar
C. Wendt
Comcast
November 2, 2020

Connected Identity for STIR
draft-peterson-stir-rfc4916-update-02

Abstract

The SIP Identity header conveys cryptographic identity information about the originators of SIP requests. The Secure Telephone Identity Revisited (STIR) framework however provides no means for determining the identity of the called party in a traditional telephone calling scenario. This document updates prior guidance on the "connected identity" problem to reflect the changes to SIP Identity that accompanied STIR, and considers a revised problem space for connected identity as a means of detecting calls that have been retargeted to a party impersonating the intended destination, as well as spoofing of mid-dialog or dialog-terminating events by intermediaries or third parties.

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.

Copyright Notice

Copyright (c) 2020 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	2
2.	Terminology	3
3.	Connected Identity Problem Statement for STIR	3
4.	Authorization Policy for Callers	5
5.	Pre-Association with Destinations	6
6.	Examples	6
7.	Updates to RFC4916	6
8.	Acknowledgments	7
9.	IANA Considerations	7
10.	Security Considerations	7
11.	Informative References	7
	Authors' Addresses	8

[1.](#) Introduction

The Session Initiation Protocol (SIP) [[RFC3261](#)] initiates sessions, and as a step in establishing sessions, it exchanges information about the parties at both ends of a session. Users review information about the calling party, for example, to determine whether to accept communications initiated by a SIP, in the same way that users of the telephone network assess "Caller ID" information before picking up calls. This information may sometimes be consumed by automata to make authorization decisions.

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](#)]). There also exists a related problem: the identity of the party who answers a call can differ from that of the initial called party for various innocuous reasons such as call forwarding, but in certain network environments it is possible for attackers to hijack the route of a called number and direct it to a resource controlled by the attacker. It can potentially be difficult to determine why a call reached a target other than the one originally intended, and whether the party ultimately reached by the call is one that the caller should trust. The property of providing identity in the backwards direction of a call is here called "connected identity."

Previous work on connected identity focused on fixing the core semantics of SIP. [\[RFC4916\]](#) allowed a mid-dialog request, such as an UPDATE [\[RFC3311\]](#), to convey identity in either direction within the context of an existing INVITE-initiated dialog. In an update to the original [\[RFC3261\]](#) behavior, [\[RFC4916\]](#) allowed that UPDATE to alter the From header field value for requests in the backwards direction: previously [\[RFC3261\]](#) required that the From header field values sent in requests in the backwards direction reflect the To header field value of the dialog-forming request, for various backwards-compatibility reasons. In other words, if Alice sent a dialog-forming request to Bob, then under the original [\[RFC3261\]](#) rules, even if Bob's SIP service forwarded that dialog-forming request to Carol, Carol would still be required to put Bob's identity in the From header field value in any mid-dialog requests in the backwards direction.

One of the original motivating use cases for [\[RFC4916\]](#) was the use of connected identity with the SIP Identity [\[RFC4474\]](#) header field. While a mid-dialog request in the backwards direction (e.g. UPDATE) can be signed with Identity like any other SIP request, forwarded requests would not be signable without the ability to change the mid-dialog From header field value: Carol, say, would not be able to furnish a key to sign for Bob's identity, if Carol wanted to sign requests in the backwards direction. Carol would however be able to sign for her own identity in the From header field value, if mid-dialog requests in the backwards direction were permitted to vary from the original To header field value.

With the obsolescence of [\[RFC4474\]](#) by [\[RFC8224\]](#), this specification updates [\[RFC4916\]](#) to reflect the changes to the SIP Identity header and the revised problem space of STIR. It also explores some new features that would be enabled by connected identity for STIR, including the use of connected identity to prevent route hijacking and to notify callers when an expected called party has successfully been reached. This document also addresses concerns about applying [\[RFC4916\]](#) connected identity to STIR as given in [\[RFC8862\]](#).

2. Terminology

In this document, the key words "MAY", "MUST", "MUST NOT", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [\[RFC2119\]](#).

3. Connected Identity Problem Statement for STIR

The STIR problem statement [\[RFC7340\]](#) enumerates robocalling, voicemail hacking, vishing, and swatting as problems with the modern telephone network that are enabled, or abetted, by impersonation: by

the ability of a calling party to arbitrarily set the telephone number that will be rendered to end users to identify the caller.

Today, sophisticated adversaries can redirect calls on the PSTN to destinations other than the intended called party. For some call centers, like those associated with financial institutions, healthcare, and emergency services, an attacker could hope to gain valuable information about people or to prevent some classes of important services. Moreover, on the Internet, the lack of any centralized or even federated routing system for telephone numbers has resulted in deployments where the routing of calls is arbitrary: calls to telephone numbers might be unceremoniously dumped on a PSTN gateway, they might be sent to a default intermediary that makes forwarding decisions based on a local flat file, various mechanisms like private ENUM might be consulted, or routing might be determined in some other, domain specific way. In short, there are numerous attack surfaces that an adversary could explore to attempt to redirect calls to a particular number to someplace other than the intended destination.

Another motivating use case for connected identity is mid-dialog requests, including BYE. The potential for an intermediary to generate a forged BYE in the backwards direction has always been built-in to the stateful dialog management of SIP. There is a class of mobile fraud attacks ("short-stopping") that rely on intermediary networks making it appear as if a call has terminated to one side, while maintaining that the call is still active to the other, in order to create a billing discrepancy that could be pocketed by the intermediary. If BYE requests in both directions of a SIP dialog could be authenticated with STIR, just like dialog-forming requests, then another impersonation vector leading to fraud in the telephone network could be shut down.

There are however practical limits to what securing the signaling can achieve. [\[RFC4916\]](#) rightly observed that once a SIP call has been answered, the called party can be replaced by a different party with a different identity due to call transfer, call park and retrieval, and so on. In some cases, due to the presence of a back-to-back user agent, it can be effectively impossible for the calling party to know that this has happened. The problem statement considered for STIR focuses solely on signaling, not whether media from the connected party should be rendered to the caller when a dialog has been established. This specification does not consider further any threats that arise from a substitution of media.

4. Authorization Policy for Callers

In a traditional telephone call, the called party receives an alerting signal and can make a decision about whether or not to pick up a phone. They may have access to displayed information, like "Caller ID", to help them arrive at an authorization decision. The situation is more complicated for callers, however: callers typically expect to be connected to the proper destination and are often holding telephones in a position that would not enable them to see displayed information, if any were available for them to review--and moreover, their most direct response to a security breach would be to hang up the call they were in the middle of placing.

While this specification will not prescribe any user experience associated with placing a call, it assumes that callers might have some way to set an authorization posture that will result in the right thing happening when the connected identity is not expected. This is analogous to a situation where SRTP negotiation fails because the keys exchanged at the media layer do not match fingerprints exchanged at the signaling layer: when a user requests confidentiality services, and they are unavailable, media should not be exchanged. Thus we assume that users have a way in their interface to require this criticality, on a per-call basis, or perhaps on a per-destination basis. Similarly, users will not always place calls where the connected identity is crucial--but when they do, they should have a way to tell their devices that the call should not be completed if it arrives at an unexpected party.

Ultimately, authorization policy for called parties is difficult to set, as calls can end up at unexpected places for legitimate reasons. Some work has been done to make sure that secure diversion works with STIR, in for example [[I-D.ietf-stir-passport-divert](#)]. Those indications can be consumed by on the terminating side by verification services to determine that a call has reached its eventual destination for the right reasons. The only way those diversion PASSporTs will be seen by the calling party is if redirection is used (SIP 3XX responses) instead of retargeting; while some network policies may want to conceal service logic from the originating party, sending redirections in the backwards direction is the only current defined way for secure indications of redirection to be revealed to the calling party. That in turn would allow the calling user agent to have a strong assurance that legitimate entities in the call path caused the request to reach a party that the caller did not anticipate.

5. Pre-Association with Destinations

Any connected identity mechanism will work best if the user knows before initiating a call that connected identity is supported by the destination side. Not every institution that a user wants to connect to securely will support STIR and connected identity out of the gate.

The user interface of modern smartphones support an address book from which users select telephone numbers to dial. Even when dialing a number manually, the interface frequently checks the address book and will display to users any provisioned name for the target of the call if one exists. Similarly, when clicking on a telephone number viewed on a web page, or similar service, smartphone often prompt users approve the access to the outbound dialer. These sorts of decision points, when the user is still interacting with the user interface, provide an opportunity to form a pre-association with the destination, and potentially even to exchange STIR PASSporTs in order to validate whether or not the expected destination can be reached securely. Again, this is probably most meaningful for contacting financial, government, or emergency services, for cases where reaching an unintended destination may have serious consequences.

Future versions of this specification will explore how the security features of destinations can be discovered before calls are set up so that calling parties can make more informed authorization decisions. This may rely on the establishment of a provisional, media-less SIP dialog which can then negotiate media when the user approves of the destination. In some environments, that may require the use of mechanisms defined by [[I-D.ietf-stir-oob](#)].

6. Examples

[TBD: Revise [RFC4916](#) examples to show new Identity header present in UPDATE and in a backwards-direction BYE.]

7. Updates to [RFC4916](#)

[TBD - ways that UPDATES in the backwards direction can carry additional information in support of the above]

In general, the guidance of [RFC4916](#) remains valid for [RFC8224](#).

The deprecation of the Identity-Info header has a number of implications for [RFC4916](#); all of the protocol examples need to be updated to reflect that.

8. Acknowledgments

We would like to thank YOU for your contributions to this specification.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

TBD.

11. Informative References

[I-D.ietf-modern-problem-framework]

Peterson, J. and T. McGarry, "Modern Problem Statement, Use Cases, and Framework", [draft-ietf-modern-problem-framework-04](#) (work in progress), March 2018.

[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-modern-teri]

Peterson, J., "An Architecture and Information Model for Telephone-Related Information (TeRI)", [draft-peterson-modern-teri-04](#) (work in progress), March 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>>.

- [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>>.
- [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>>.
- [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>>.
- [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>>.

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

