SIPCORE
Internet-Draft
Intended status: Standards Track
Expires: March 1, 2020

H. Schulzrinne
Columbia University

August 29, 2019

SIP Call-Info Parameters for Labeling Calls draft-ietf-sipcore-callinfo-spam-04

Abstract

Called parties often wish to decide whether to accept, reject or redirect calls based on the likely nature of the call. For example, they may want to reject unwanted telemarketing or fraudulent calls, but accept emergency alerts from numbers not in their address book. This document describes SIP Call-Info parameters and a feature tag that allow originating, intermediate and terminating SIP entities to label calls as to their type, confidence and references to additional information.

Table of Contents

1. Introduction 2
2. Normative Language 3
3. Overview of Operation 4
4. Parameters 4
5. Call Types 5
6. Examples 7
6.1. REGISTER Response 7
6.2. INVITE Request 7
7. ABNF 7
8. IANA Considerations 8
8.1. SIP Call-Info Header Field Parameters 8
8.2. SIP Global Feature-Capability Indicator 8
8.3. SIP Call-Info Type Parameter 8
9. Security Considerations 9
10. Acknowledgements 9
11. References 10
11.1. Normative References 10
11.2. Informative References 11
Author's Address 11

1. Introduction

In many countries, an increasing number of calls are unwanted [RFC5039], as they might be fraudulent, telemarketing or the receiving party does not want to be disturbed by, say, surveys or solicitation by charities. Currently, called parties have to rely exclusively on the caller's number or, if provided, caller name, but unwanted callers may not provide their true name or may use a name that misleads, e.g., "Cardholder Services". On the other hand, many calls from unknown numbers may be important to the called party, whether this is an emergency alert from their emergency management office or a reminder about a doctor's appointment. Since many subscribers now reject all calls from unknown numbers, such calls may also inadvertently be left unanswered. Users may also install smartphone apps that can benefit from additional information in making decisions as to whether to ring, reject or redirect a call to voicemail.

To allow called parties to make more informed decisions on how to handle incoming calls from unknown callers, we describe a new set of parameters for the SIP [RFC3261] Call-Info header field for labeling the nature of the call.

This specification assumes that the user agent can trust its SIP provider to correctly label the nature of calls. This may not always be the case and not all SIP service providers will label calls, so users may need to draw on other, third-party, sources of call information beyond the scope of this specification or may decide to disregard the call labeling offered by their service provider. (Service providers may, for example, be reluctant to label calls as spam.) However, the SIP registrar already occupies a position of trust by necessity; also, the user agent is typically a customer of the operator of the registrar or within the same organization, e.g., if the registrar is part of a PBX. Thus, the entity inserting the Call-Info header field and the UAS relying on it SHOULD be part of the same trust domain [RFC3324]. Conversely, the entity signing the caller information [RFC8224] is likely either to be the caller itself or the originating service provider, neither of which is likely to label the caller as a category unlikely to be answered by the called party.

The service provider inserting the Call-Info header field may draw on a wide variety of sources. For example, service providers offering alerting or notification services (e.g., for packages or health alerts) may register their phone numbers, after suitable vetting, in shared databases. Government agencies could publish electronic directories of official telephone numbers, drawing on the historical precedent of the "blue pages" found in printed phone directories. Government regulators for financial services, health care providers and charitable organizations could provide sources of telephone numbers and service types belonging to such organizations. Finally, crowd-sourcing might also be used to populate databases of call types. In the United States, industry organizations have proposed variations of such caller databases to prevent accidental blocking of calls based on their statistics such as frequency or duration alone.

Providers may also find the SIP Priority header ([RFC3261], Section 20.26) field useful in helping called parties decide how to respond to an incoming call.

2. Normative Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Overview of Operation

This document describes a new set of optional parameters and usage for the SIP [RFC3261] Call-Info header field, with a purpose "info", for labeling the nature of the call. The header field may be inserted by the call originator, an intermediate proxy or B2BUA or the terminating carrier, based on assertions by the caller, number-indexed databases, call analytics or other sources of information. The SIP provider serving the called party MUST remove any parameters enumerated in this specification that it does not trust.

To ensure that an untrusted originating caller does not mislead the called party, a new feature capability indicator [RFC6809], sip.call-info.spam, in the REGISTER response signals whether the terminating carrier supports the feature described in this document and thus will remove any untrusted 'confidence', 'origin', 'source' and 'type' Call-Info header field information parameters. It is possible for the terminating carrier to support this feature by simply removing all parameters defined in the document, without inserting any of its own information, although this is likely to be unusual. A user agent MUST ignore any of the parameters defined in this document unless the feature capability indicator is present in the response to the REGISTER request. An example of the REGISTER response is shown in Section 6.1.

SIP proxies or B2BUAs MUST add a new Call-Info "info" header field value, rather than add parameters to an existing value. Thus, one SIP request MAY contain several Call-Info header instances of purpose "info", either as a single header with a comma-separated list of header values or separate headers, or some combination.

As defined in [RFC3261], the Call-Info header field contains a URI that can provide additional information about the caller or call. For example, many call filtering services provide a web page with crowd-sourced information about the calling number. If the entity inserting the header field does not have information it wants to link to, it MUST use an empty data URL [RFC2397] as a placeholder, as in "data:,". (The Call-Info header field syntax makes the URI itself mandatory.) An example is shown in Section 6.2.

4. Parameters

All of the parameters listed below are optional and may appear in any combination and order. Their ABNF is defined in Section 7. All except the 'type' parameter are optional.

confidence The 'confidence' parameter carries an estimated probability that the call is of the nature indicated in the 'type'

parameter, expressed as a whole-number percentage between 0 and 100, inclusive, with larger numbers indicating higher probability. The computation of the estimate is beyond the scope of this specification. If a 'type' is not specified, this parameter estimates the likelihood that the call is unwanted spam by the called party. If the confidence level is not specified, the sender considers the information reliable enough to act on, according to its local decision thresholds.

origin The origin parameter provides free-text information, as a quoted-text (UTF8-encoded) string, about the source of the 'type' or 'confidence' parameter and is meant to be used for debugging, rather than for display to the end user. For example, it may indicate the name of an external information source, such as a list of known emergency alerters or a government agency.

source The source parameter identifies the entity, by host name, domain or IP address, that inserted the 'confidence', 'origin' and 'type' parameters. It uses the "host" ABNF syntax.

type The type parameter indicates the type of the call or caller. It is drawn from an extensible set of values, with the initial set listed below. Gateways to analog phone systems MAY include the label in caller name (CNAM) information delivered to user equipement. Automated call classification systems MAY use this information as one factor in deciding how to handle the call. Calls SHOULD be labeled with types that may make it more likely that the caller will answer (e.g., for alert and health-related calls) if the entity inserting the information is confident that the calling party number is valid, e.g., because the request has been signed [RFC8224].

5. Call Types

The following initial set of types are defined. The call types are generally based on the caller's telephone number or possibly an assertion by a trusted caller, as the content cannot be not known. Each call is tagged with at most one type label, i.e., the labels are meant to be mutually exclusive. The definitions are meant to be informal and reflect the common understanding of subscribers who are not lawyers. By their very nature, this classification may sometimes be erroneous, e.g., if a number has been re-assigned to another entity or if crowd-sourced information is wrong, and thus should be treated as a hint or estimate. Each entity inserting type information will need to define its own policy as to the level of certainty it requires before it inserts type information.

Other strings may be used; there does not appear to be a need for defining vendor-defined strings as the likelihood of confusion between a service-provider-specific usage and a later extension to the list appears low. Additional labels are registered with IANA.

business Calls placed by businesses, i.e., an entity or enterprise entered into for profit. This type is used if no other, more precise, category fits.

debt-collection Calls related to collecting of debt owed or alleged to be owed by the called party.

emergency-alert Calls that provide the recipient warnings and alerts regarding a pending or on-going emergency. (This call type is unrelated to emergency calls placed by individuals using emergency numbers such as 9-1-1 or 1-1-2.)

fraud The call is considered to be fraudulent.

government A call placed by a government entity, if no more specific label such as "health" or "debt-collection" is known or applies.

health Informational calls by health plans, health care clearinghouses or health care provider, where health care means care, services, or supplies related to the health of an individual.

informational Calls intended to convey information to the called party about a transaction such as package delivery, appointment reminder, or order confirmation.

not-for-profit A call placed by a not-for-profit organization, including for soliciting donations or providing information.

personal A non-business, person-to-person, call, e.g., from a residential line or personal mobile number.

political Calls related to elections or other political purposes.

public-service Calls that provide the recipient information regarding public services, e.g., school closings.

prison Calls from jails, prisons and other correctional facilities.

spam A call that is likely unwanted, if not otherwise classified.

spoofed The calling number for this call has been spoofed. (For example, the call has failed STIR validation [RFC8224] within the

SIP service provider network or the telephone number is not a valid number or is known not to have been assigned.)

survey A call that solicits the opinions or data of the called party.

telemarketing Calls placed in order to induce the purchase of a product or service to the called party.

trusted The call is being placed by a trusted entity and falls outside the other categories listed. This may include call backs, e.g., from a conferencing service, or messages from telecommunication carriers and utilities.

6. Examples

6.1. REGISTER Response

The example below shows a partial REGISTER response showing that the registrar and proxy will remove any untrusted Call-Info header elements.

```
SIP/2.0 200 OK
...
From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl
To: Bob <sips:bob@biloxi.example.com>;tag=34095828jh
...
Feature-Caps: *; +sip.call-info.spam
```

6.2. INVITE Request

```
INVITE sip:alice@example.com SIP/2.0
...
Call-Info: <http://wwww.example.com/5974c8d942f120351143>
  ;source=carrier.example.com
  ;purpose=info ;confidence=85 ;type=fraud
  ;origin="FTC fraud list"
```

7. ABNF

```
               label-info-params = [ci-confidence] / [ci-source] / [ci-
origin] / ci-type
               ci-confidence = "confidence" EQUAL 1*3DIGIT
               ci-origin = "origin" EQUAL quoted-string
               ci-source = "source" EQUAL host
               ci-type = "type" EQUAL ("business" / "debt-collection" /
"emergency-alert" / "fraud" /
                           "government" / "health" / "informational" / "not-
for-profit" /
                           "personal" / "political" / "public-service" /
"prison" / "spam" /
                           "spoofed" / "survey" / "telemarketing" /
"trusted" /
                           iana-token)
```

8. IANA Considerations

8.1. SIP Call-Info Header Field Parameters

This document defines the 'confidence', 'origin', 'source' and 'type' parameters in the Call-Info header in the "Header Field Parameters and Parameter Values" registry defined by [RFC3968].

Header Field	Parameter Name	Predefined Values	Reference
[this RFC]	Call-Info	confidence	No
Call-Info	origin	No	[this RFC]
Call-Info	source	No	[this RFC]
Call-Info	type	Yes	[this RFC]

8.2. SIP Global Feature-Capability Indicator

This document defines the feature capability sip.call-info.spam in the "SIP Feature-Capability Indicator Registration Tree" registry defined in [RFC6809].

Name sip.call-info.spam

Description This feature-capability indicator when used in a REGISTER response indicates that the server will add, inspect, alter and possibly remove the Call-Info header field parameters defined in the reference.

Reference [this RFC]

8.3. SIP Call-Info Type Parameter

This specification establishes the "Call-Info Type" sub-registry under http://www.iana.org/assignments/sip-parameters. Call-Info "type" parameters are used in the "type" parameter in the SIP Call-Info header field. The initial values are listed in Section 5.

Additional values are allocated by expert review [RFC5226]; only the token value, using the ABNF iana-token, and a brief description, typically no more than a few sentences, is required. The ABNF for iana-token is defined in [RFC3261]. A specification is not required.

9. Security Considerations

The security considerations in [RFC3261] (Section 20.9) apply. A user agent MUST ignore the parameters defined in this document unless the SIP REGISTER response contained the sip.call-info.spam feature capability. B2BUAs or proxies that maintain user registrations MUST remove any parameters defined in this document that were provided by untrusted third parties.

The UAS SHOULD only consider Call-Info header field information that originates from a registrar that is part of the same trust domain [RFC3324].

The protection offered against rogue SIP entities by the feature capability relies on protecting the REGISTER response against man-in-the-middle attacks that maliciously add the capability indicator. Thus, a UAS SHOULD NOT trust the information in the "Call-Info" header field unless the SIP session between the entity inserting the header field and the UAS is protected by TLS [RFC8446].

Labeling calls is likely only useful if the caller identity can be trusted, e.g., by having the call signaling requests signed [RFC8224], as otherwise spoofed calls would likely be mislabeled and thus increase the likelihood that the called party is mislead, answers unwanted calls or is defrauded. Thus, this information MUST only be added calls with an attestation level of "Full Attestation" [RFC8588] or for calls where the SIP entity inserting the header knows to have correct calling number information, e.g., because the call originated within the same PBX or the same carrier and the operating entity ensures that caller ID spoofing is highly unlikely within their realm of responsibility.

10. Acknowledgements

Jim Calme and other members of the Robocall Strikeforce helped draft the initial list of call types. Tolga Asveren, Ben Campbell, Keith Drage, Christer Holmberg, Paul Kyzivat and Dale Worley provided helpful comments on the document.

11. References

11.1. 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>.

[RFC2397] Masinter, L., "The "data" URL scheme", RFC 2397, DOI 10.17487/RFC2397, August 1998, <https://www.rfc-editor.org/info/rfc2397>.

[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>.

[RFC3324] Watson, M., "Short Term Requirements for Network Asserted Identity", RFC 3324, DOI 10.17487/RFC3324, November 2002, <https://www.rfc-editor.org/info/rfc3324>.

[RFC3968] Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)", BCP 98, RFC 3968, DOI 10.17487/RFC3968, December 2004, <https://www.rfc-editor.org/info/rfc3968>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

[RFC6809] Holmberg, C., Sedlacek, I., and H. Kaplan, "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)", RFC 6809, DOI 10.17487/RFC6809, November 2012, <https://www.rfc-editor.org/info/rfc6809>.

[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>.

[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>.

11.2. Informative References

[RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", RFC 5039, DOI 10.17487/RFC5039, January 2008, <https://www.rfc-editor.org/info/rfc5039>.

[RFC8588] Wendt, C. and M. Barnes, "Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)", RFC 8588, DOI 10.17487/RFC8588, May 2019, <https://www.rfc-editor.org/info/rfc8588>.

Author's Address

Henning Schulzrinne
Columbia University
450 Computer Science Bldg.
New York, NY 10027
US

Email: hgs@cs.columbia.edu