SIPCORE
Internet-Draft
Updates: RFC6442 (if approved)
Intended status: Standards Track
Expires: March 19, 2020

J. Winterbottom
Winterb Consulting Services
R. Jesske
Deutsche Telekom
B. Chatras
Orange Labs
A. Hutton
Atos

September 16, 2019

Location Source Parameter for the SIP Geolocation Header Field
draft-ietf-sipcore-locparam-03.txt

Abstract

There are some circumstances where a Geolocation header field may contain more than one location value. Knowing the identity of the node adding the location value allows the recipient more freedom in selecting the value to look at first rather than relying solely on the order of the location values. This document defines the location-source parameter so that the entity adding the location value to Geolocation header field can identify itself using its hostname.

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 March 19, 2020.

Copyright Notice

Table of Contents

1. Introduction

The SIP Geolocation specification [RFC6442] describes the "Geolocation" SIP header field which is used to indicate that the SIP message is conveying location information. [RFC6442] specifies that SIP intermediaries should not add location values to a SIP request that already contains location value. [RFC6442] also states that if a SIP intermediary adds location it is fully responsible for addressing the concerns of any 424 (Bad Location Information) SIP response it receives. However, some communications architectures, such as 3GPP [TS23-167] and ETSI [M493], prefer to use information provided by edge-proxies or acquired through the use of core-network nodes, before using information provided solely by user equipment (UE). These solutions don't preclude the use of UE provided location but require a means of being able to distinguish the identity of the node adding the location value to the SIP message from that provided by the UE.

[RFC6442] stipulates that the order of location values in the Geolocation header field is the same as the order in which they were added to the header field. Whilst this order provides guidance to the recipient as to which values were added to the message earlier in the communication chain, it does not provide any indication of which node actually added the location value. Knowing the identity of the entity that added the location to the message allows the recipient to choose which location to consider first rather than relying solely on the order of the location values in the Geolocation header field.

This document extends the Geolocation header field, by allowing an entity adding the location value to identity itself using a hostname. This is done by defining a new geoloc-param header field parameter, location-source."How the entity adding the location value to the header field obtains the location information is out of scope of this document.

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. Rationale

The primary intent of the location-source parameter in this specification is for use in emergency calling. There are various architectures defined for providing emergency calling using SIP-based

messaging. Each has it own characteristics with corresponding pros and cons. All of them allow the UE to provide location information, however, many also attach other sources of location information to support veracity checks, provide backup information, or to be used as the primary location.

This document makes no attempt to comment on these various architectures or the rationale for them wishing to include multiple location values. It does recognize that these architectures exist and that there is a need to identify the entity adding the location information.

The location-source parameter adds the location source generating the location value to increase the trustworthiness of the location information.

The location-source parameter is applicable within a single private administrative domain or between different administrative domains where there is a trust relationship between the domains. Thus it is intended to use this parameter only in trust domains where Spec(T) as described in [RFC3325] exists.

The location-source parameter is not included in a SIP message sent to another network if there is no trust relationship. The The location-source parameter is not applicable if the administrative domain manages emergency calls in a way that does not require any generation of the location.

The functional architecture described within ETSI [M493] is an example of architecture where this parameter makes sense to be used.

4. Mechanism

The mechanism employed adds a parameter to the location value defined in [RFC6442] that identifies the hostname of the entity adding the location value to the Geolocation header field. The Augmented BNF (ABNF) [RFC5234] for this parameter is shown in Figure 1.

```
location-source = "loc-src" EQUAL hostname
hostname = <defined in RFC3261>
```

Figure 1: Location Source

Only a fully qualified host name is valid. The syntax does not support IP addresses, and if an entity conforming to this specification receives a Geolocation header field with a location-source parameter containing an IP address then the parameter MUST be removed.

A SIP intermediarity conformant to this specification adding a location value to a Geolocation header field SHOULD also add a location-source header field parameter so that it is clearly identified as the node adding the location. A UA MUST NOT insert a location-source header field parameter. If a SIP intermediarity receives a message from an untrusted source with the location-source parameter set then it MUST remove the location-source parameter before passing the message into a trusted network.

5. Example

The following example shows a SIP INVITE message containing a Geolocation header field with two location values. The first location value points to a PIDF-LO in the SIP body using a content-indirection (cid:) URI per [RFC4483] and this is provided by the UE. The second location value is an https URI the provided by a SIP intermediarity which identifies itself using the location-source parameter.

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bK74bf9
Max-Forwards: 70
To: Bob <sip:bob@biloxi.example.com>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Geolocation: <cid:target123@atlanta.example.com>,
     <https://lis.example.com:8222/y77syc7cuecbh>;
              loc-src=edgeproxy.example.com
Geolocation-Routing: yes
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...
```

Figure 2: Example Location Request.

6. Privacy Considerations

This document doesn't change any of the privacy considerations described in [RFC6442]. While the addition of the location-source parameter does provide an indicator of the entity that added the

location in the signaling path this provides little more exposure than a proxy identity being added to the record-route header field.

7. Security Considerations

This document introduces the ability of a SIP intermediarity to insert a host name indicating that they added the specific location value to the Geolocation header field. The intent is for this field to be used by the location recipient in the event that the SIP message contains multiple location values. As a consequence this parameter should only be used by the location recipient in a trusted network.

As already stated in [RFC6442] securing the location hop- by-hop, using TLS, protects the message from eavesdropping and modification in transit, but exposes the information to all SIP intermediaries on the path as well as the endpoint. The location-source parameter is applicable within a single private administrative domain or between different administrative domains where there is a trust relationship between the domains. If such trust domain is not given it is strongly recommended to delete the location information.

The use of this parameter is not restricted to a specific architecture but using multiples locations and loc-src may end in compatibility issues. [RFC6442] already addresses the issue of multiples locations. To avoid problems of wrong interpretation of loc-src the value may be removed when passed to an other domain.

8. IANA Considerations

8.1. Registration of location-source parameter for Geolocation header field

This document calls for IANA to register a new SIP header parameter as per the guidelines in [RFC3261], which will be added to header sub-registry under http://www.iana.org/assignments/sip-parameters.

Header Field: Geolocation

Parameter Name: loc-src

9. Acknowledgements

The authors would like to thank Dale Worley and Christer Holmberg for their extensive review of the draft The authors would like to acknowledge the constructive feedback provided by Paul Kyzivat and Robert Sparks.

10. References

10.1. 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>.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, DOI 10.17487/RFC3325, November 2002, <https://www.rfc-editor.org/info/rfc3325>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, DOI 10.17487/RFC6442, December 2011, <https://www.rfc-editor.org/info/rfc6442>.

[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>.

10.2. Informative References

[M493] European Telecommunications Standards Institute, "Functional architecture to support European requirements on emergency caller location determination and transport", ES 203 178, V 1.1.1, Februar 2015.

[RFC4483] Burger, E., Ed., "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", RFC 4483, DOI 10.17487/RFC4483, May 2006, <https://www.rfc-editor.org/info/rfc4483>.

[TS23-167]
3rd Generation Partnership Project, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions", TS 23.167, V 12.1.0, March 2015.

Authors' Addresses

James Winterbottom
Winterb Consulting Services
Gwynneville, NSW 2500
AU

Phone: +61 448 266004
Email: a.james.winterbottom@gmail.com

Roland Jesske
Deutsche Telekom
Heinrich-Hertz Str, 3-7
Darmstadt 64295
Germany

Email: r.jesske@telekom.de
URI: www.telekom.de

Bruno Chatras
Orange Labs
38-40 rue du General Leclerc
Issy Moulineaux Cedex 9 F-92794
France

Email: bruno.chatras@orange.com

Andrew Hutton
Atos
Mid City Place
London WC1V 6EA
UK

Email: andrew.hutton@atos.net