Location Source Parameter for the SIP Geolocation Header Field
draft-ietf-sipcore-locparam-04

Abstract

   There are some circumstances where a Geolocation header field may
   contain more than one locationValue. Knowing the identity of the
   node adding the locationValue allows the recipient more freedom in
   selecting the value to look at first rather than relying solely on
   the order of the locationValues. This document defines the "loc-src"
   parameter so that the entity adding the locationValue to Geolocation
   header field can identify itself using its hostname. This document
   updates RFC 6442.

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 April 10, 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 locationValues to a SIP request
that already contains locationValue. [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 locationValue to the SIP message from that provided by the
UE.

[RFC6442] stipulates that the order of locationValues 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 identify which node added the
locationValue. 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
locationValues in the Geolocation header field.

This document extends the Geolocation header field, by allowing an
entity adding the locationValue to identity itself using a hostname.
This is done by defining a new geoloc-param header field parameter,
"loc-src"."How the entity adding the locationValue 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 "loc-src" 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 does not comment on these various architectures or on
the rationale for including multiple locationValues. It does
recognize that these architectures exist and that there is a need to
identify the entity adding the location information.

The "loc-src" parameter adds the location source generating the
locationValue to increase the trustworthiness of the location
information.

The "loc-src" 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 "loc-src" parameter is not included in a SIP message sent to
another network if there is no trust relationship. The "loc-src"
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 an architecture where it makes sense to use this
parameter.

4. Mechanism

The mechanism adds a geoloc-param parameter to the locationValue
defined in [RFC6442] that identifies the hostname of the entity
adding the locationValue 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 "loc-src"
parameter containing an IP address then the parameter MUST be
removed.

A SIP intermediary conformant to this specification adding a
locationValue to a Geolocation header field SHOULD also add a "loc-
src" header field parameter so that it is clearly identified as the
node adding the location. A UA MUST NOT insert a "loc-src" header
field parameter. If a SIP intermediary receives a message from an
untrusted source with the "loc-src" parameter set then it MUST remove
the "loc-src" 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 locationValues. The first
locationValue 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 locationValue is an https URI provided by a SIP
intermediary which identifies itself using the "loc-src" 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 "loc-src"
parameter identifies the entity that added the location in the

   signaling path, this addition provides little more exposure than
   adding a proxy identity to the Record-Route header field.

7. Security Considerations

   This document introduces the ability of a SIP intermediary to insert
   a host name indicating that they added the specific locationValue 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 locationValues. 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 "loc-src" 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 with misinterpretation of the
   "loc-src" parameter, the value may be removed when passed to an other
   domain.

8. IANA Considerations

8.1. Registration of loc-src parameter for Geolocation header field

   The IANA is asked to add a new SIP header field parameter for the
   Geolocation header field in the "Header Field Parameters and
   Parameter Values" subregistry (created by [RFC3968]) of the "Session
   Initiation Protocol (SIP) Parameters" registry found at
   https://www.iana.org/assignments/sip-parameters/.

   Header Field: Geolocation

   Parameter Name: loc-src

   Predefined Values: No

   Reference: this RFC

9. Acknowledgements

The authors would like to thank Dale Worley, Christer Holmberg and
Jean Mahoney 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>.

[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>.

[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>.

[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
   44, avenue de la Republique
   Chatillon   F-92320
   France

   Email: bruno.chatras@orange.com

   Andrew Hutton
   Atos
   Mid City Place
   London WC1V 6EA
   UK

   Email: andrew.hutton@atos.net