ECRIT
Internet-Draft
Intended status: Informational
Expires: August 25, 2010

H. Schulzrinne
Columbia University
L. Liess
Deutsche Telekom
H. Tschofenig
Nokia Siemens Networks
B. Stark
AT&T
A. Kuett
Skype

February 21, 2010

Location Hiding: Problem Statement and Requirements
draft-ietf-ecrit-location-hiding-req-04.txt

Abstract

The emergency services architecture developed in the IETF Emergency Context Resolution with Internet Technology (ECRIT) working group describes an architecture where location information is provided by access networks to end points or VoIP service providers in order to determine the correct dial string and information to route the call to a Public Safety Answering Point (PSAP). For determining the PSAP Uniform Resource Identifier (URI) the usage of the Location-to-Service Translation (LoST) Protocol is envisioned.

This document provides a problem statement and lists requirements for situations where the Internet Access Provider (IAP) and/or the Internet Service Provider (ISP) are only willing to disclose limited or no location information.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at

http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 25, 2010.

Copyright Notice

Table of Contents

1. Introduction

1.1. Emergency Services Architecture

The emergency services architecture developed in the IETF Emergency Context Resolution with Internet Technology (ECRIT) working group, see [I-D.ietf-ecrit-framework], describes an architecture where location information is provided by access networks to end points or VoIP service providers in order to determine the correct dial string and information to route the call to a Public Safety Answering Point (PSAP). The Location-to-Service Translation (LoST) Protocol [RFC5222] allows callers and other call-routing entities to determine the PSAP Uniform Resource Identifier (URI) for a specific geographical location together with a service URI [RFC5031]. The basic architecture is shown in Figure 1 of [I-D.ietf-ecrit-framework] and further detailed in the message flow in Figure 2 of [I-D.ietf-ecrit-framework].

For emergency services, location information is needed in three ways:

1. Emergency call routing to the PSAP that is responsible for a specific geographical region
2. Dispatch of the emergency personnel to the scene of an accident, crime or other types of incidents
3. Additionally, a Voice Service Provider (VSP) may need to verify that an call is indeed an emergency call and may therefore require location information to ensure that calls routed to a specific URI point to a PSAP.

This document focuses on item (1) and item (3). Providing location

information by the ISP to the PSAP and to the emergency personnel are typically legal obligations covered by regulatory frameworks.

1.2. Location Hiding

Internet Access Providers (IAPs) and Internet Service Providers (ISPs)) typically have little incentives to provide location information to end hosts or independent VSPs (without monetary compensation) for any purpose, including for emergency call routing. The decision to deny disclosure of location information can be driven by a number of technical and business concerns. Some providers may perceive a risk that allowing users to access location information for non-emergency purposes or prior to an emergency call will incur additional server load and thus costs. Other providers may not want to make location information available without the ability to charge for it. Yet others fear problems with regard to privacy when disclosing location information to potentially unknown third parties.

1.3. Location by Reference

The work on the Location Configuration Protocol (LCP) indicated the need to provide the capability to obtain Location-by-References (LbyRs) in addition to Location-by-Value (LbyV) from a Location Information Server (LIS).

The LCP problem statement and requirements document can be found in [I-D.ietf-geopriv-l7-lcp-ps]. The requirements for obtaining an LbyR via the LCP and the corresponding dereferencing step can be found in [I-D.ietf-geopriv-lbyr-requirements].

HTTP Enabled Location Delivery (HELD), see [I-D.ietf-geopriv-http-location-delivery], is an instantiation of the LCP concept and allows LbyVs and LbyRs to be requested.

A location reference may already satisfy the requirement for location hiding if the PSAP has the appropriate credentials to resolve the reference. These credentials allow the ISP/IAP to authenticate and to authorize the party that would like to request location information. The policy to obtain these credentials allows ISPs/IAPs to put constraints under which these credentials are handed out.

ISP/IAPs ideally might want to engage in a business relationship with the VSP to receive a financial compensation for the service they provide. On the Internet the number of VSPs is potentially large and the VSPs would not want to enter a business contract with potentially every ISP/IAP worldwide. The number of potential contracts between ISPs/IAPs and PSAPs is, however, relatively small as they typically need to have a local relationship as PSAPs provide their emergency services support in a certain geographical region for which certain ISPs/IAPs have networks deployed.

Note that the requirement being met here is for delivery of location information to the PSAP, not for LoST routing or for validation at the VSP. Another obstacle when it comes to the usage of location reference for location-based routing from a technical point of view is that a location reference cannot be used as input to LoST [RFC5222], as LoST requires location per value rather than a reference. Also, LoST servers may be operated by independent parties, including VSPs, which again may not be able to resolve the reference to location by value. (Note that LoST is a protocol used for determining the location-appropriate PSAP based on location information and a Service URN [RFC5031].

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119], with the important qualification that, unless otherwise stated, these terms apply to the design of an solution supporting location hiding, not its implementation or application.

This document reuses terminology from [I-D.ietf-geopriv-l7-lcp-ps].

3. Requirements

Req-1: There MUST be a way for the ISP/IAP to withhold precise location information from the endpoint and from the VSP.

Req-2: The ISP/IAP MUST support the ability of the endpoint or the

VSP to route emergency calls.

Req-3: The VSP MUST be able to validate that a call purported to be an emergency call is being routed to a bona fide URI, which is denoted by being a URI in LoST for the designated emergency service. This requirement is provided to deal with potential security problems described in Section 5.1 of [RFC5069].

Req-4: The PSAP MUST receive precise location information (by value) about emergency callers. As such, any solution MUST be able to provide location information to the PSAP even while withholding it from the emergency caller.

Req-5: The proposed solution MUST NOT assume a business or trust relationship between the caller's VSP and the caller's ISP.

Req-6: A solution MUST consider deployment scenarios where a VSP does not operate in the same jurisdiction as the PSAP.

Req-7: The solution MUST offer automated discovery of servers and and other necessary configuration information. No manual configuration can be assumed.

Req-8: The steps needed by the endpoint for emergency calling SHOULD be no different when location is withheld vs. when location is not withheld. In particular, user agents cannot require additional configuration to discover which particular environment (hiding or no hiding) they find themselves in.

Req-9: The solution SHOULD work without the ISP/IAP having to support SIP and without the need to utilize SIP between the endpoint and the VSP.

Req-10: The solution MUST work if PSAP boundaries have holes. (For a discussion about holes in PSAP boundaries and their encoding the reader is referred to [I-D.ietf-ecrit-specifying-holes].)

Req-11: The solution MUST NOT assume the existence of Emergency Service Routing Proxies (ESRPs) per country, state and city.

Req-12: The solution MUST consider that service boundaries for

different emergency services may differ, but they overlap at the location of the caller.

Req-13: Though the solution MAY add steps to the emergency call routing process described in [I-D.ietf-ecrit-framework], these steps MUST NOT significantly increase call setup latency. For example, the revised process MUST NOT include "trial-and-error" operations on its critical path, such as attempts at LbyR resolutions that may take time to time out.

Req-14: The solution MUST allow the end host to determine PSAP/ESRP URLs prior to the call, for all emergency services.

Req-15: The solution MUST allow UAs to discover at least their dial string ahead of the emergency call.

Req-16: The solution MUST have minimal impact on UAs, i.e., a solution is preferred if it does not require an substantially different emergency services procedures compared to the procedure of dealing with emergency services where no location hiding is applied.

Req-17: The solution MUST NOT interfere with the use of LoST for non-emergency services.

Req-18: The solution MUST allow emergency calls to reach an IP-to-PSTN gateway rather than the IP-based PSAP directly.

Req-19: The solution MUST NOT shift effort (externality), i.e., the convenience of the location-hiding ISP MUST NOT impose a burden on user agents or non-hiding ISPs/IAPs and SHOULD NOT impose a burden on VSPs.

Req-20: The solution SHOULD minimize the impact on LoST, SIP conveyance [I-D.ietf-sipcore-location-conveyance] and DHCP.

Req-21: The solution SHOULD NOT break in the presence of NATs and

SHOULD consider the presence of legacy devices, as described in [I-D.ietf-geopriv-l7-lcp-ps].

4. IANA Considerations

This document does not require actions by IANA.

5. Security Considerations

This document does not raise additional security consideration beyond those mentioned in [I-D.ietf-geopriv-l7-lcp-ps] and discussed in this document.

6. Acknowledgments

We would like to thank the following ECRIT working group members (in no particular order) for their contributions:

- Andrew Newton (andy@hxr.us)
- James Winterbottom (James.Winterbottom@andrew.com)
- Brian Rosen (br@brianrosen.net)
- Richard Barnes (rbarnes@bbn.com)
- Marc Linsner (mlinsner@cisco.com)
- Ted Hardie (hardie@qualcomm.com)

The authors would also like to thank Ben Campbell for his Gen-ART review. Additionally, we would like to thank Jari Arkko, Alexey Melnikov, Tim Polk, and Dan Romascanu for their IESG review.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[I-D.ietf-geopriv-l7-lcp-ps]
Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-10 (work in progress), July 2009.

[I-D.ietf-sipcore-location-conveyance]

Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sipcore-location-conveyance-02 (work in progress), February 2010.

[I-D.ietf-ecrit-framework]
Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia", draft-ietf-ecrit-framework-10 (work in progress), July 2009.

[RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H., and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008.

[RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

[I-D.ietf-geopriv-lbyr-requirements]
Marshall, R., "Requirements for a Location-by-Reference Mechanism", draft-ietf-geopriv-lbyr-requirements-09 (work in progress), November 2009.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.

[I-D.ietf-geopriv-http-location-delivery]
Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-16 (work in progress), August 2009.

[I-D.ietf-ecrit-specifying-holes]
Winterbottom, J. and M. Thomson, "Specifying Holes in LoST Service Boundaries", draft-ietf-ecrit-specifying-holes-01 (work in progress), October 2008.

7.2. Informative References

Authors' Addresses

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7004
Email: hgs+ecrit@cs.columbia.edu
URI: http://www.cs.columbia.edu

Laura Liess
Deutsche Telekom Networks
Deutsche Telekom Allee 7
Darmstadt, Hessen 64295
Germany

Phone:
Email: L.Liess@telekom.de
URI: http://www.telekom.de

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Barbara Stark
AT&T
725 W Peachtree St, NE

Atlanta, GA 30308
USA

Phone: +1 404 499 7026
Email: barbara.stark@att.com

Andres Kuett
Skype

Email: andres.kytt@skype.net