Internet Engineering Task Force (IETF)
Request for Comments: 6444
Category: Informational
ISSN: 2070-1721

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

January 2012

Location Hiding: Problem Statement and Requirements

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 endpoints or Voice over IP (VoIP) service providers in order to determine the correct dial string and information to route the call to a Public Safety Answering Point (PSAP). To determine 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 document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6444.

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 [RFC6443], describes an architecture where location information is provided by access networks to endpoints 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 URN [RFC5031]. The basic architecture is shown in Figure 1 of [RFC6443] and further detailed in the message flow in Figure 2 of [RFC6443].

For emergency services, location information is needed for three purposes:

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 type of incident.

3. Additionally, a Voice Service Provider (VSP) may need to verify that a 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 items (1) and (3). Providing location information by the ISP to emergency authorities, including PSAPs, regional emergency management association, and emergency personnel is typically a legal obligation covered by regulatory frameworks.

1.2. Location Hiding

Internet Access Providers (IAPs) and Internet Service Providers (ISPs) typically have little incentive 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 is [RFC5687]. The requirements for obtaining an LbyR via the LCP and the corresponding dereferencing step can be found in [RFC5808].

HTTP Enabled Location Delivery (HELD), see [RFC5985], 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. ISPs/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. Since LoST [RFC5222] requires location by value, location by reference cannot be used for location-based routing. 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 [RFC5687].

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 consider that service boundaries for the various emergency services responsible for a particular location may differ.

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

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 [RFC5964].)

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 [RFC6443], 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 user agents (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 a substantially different emergency service procedure 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 [RFC6442], 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 [RFC5687].

4. Security Considerations

This document does not raise additional security consideration beyond those mentioned in [RFC5687] and discussed in this document.

5. 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.

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[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.

[RFC5687] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", RFC 5687, March 2010.

[RFC5808] Marshall, R., "Requirements for a Location-by-Reference Mechanism", RFC 5808, May 2010.

[RFC5964] Winterbottom, J. and M. Thomson, "Specifying Holes in Location-to-Service Translation (LoST) Service Boundaries", RFC 5964, August 2010.

[RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, December 2011.

[RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

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