ECRIT
Internet-Draft
Intended status: Informational
Expires: April 29, 2010

H. Schulzrinne
Columbia University
H. Tschofenig
Nokia Siemens Networks
M. Patel
Nortel

October 26, 2009

Public Safety Answering Point (PSAP) Callbacks
draft-schulzrinne-ecrit-psap-callback-01.txt

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 April 29, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

After an emergency call is completed (either prematurely terminated by the emergency caller or normally by the call-taker) it is possible that the call-taker feels the need for further communication or for a clarification. For example, the call may have been dropped by accident without the call-taker having sufficient information about the current situation of a wounded person. A call-taker may trigger a callback towards the emergency caller using the contact information provided with the initial emergency call. This callback could, under certain circumstances, then be treated like any other call and as a consequence, it may get blocked by authorization policies or may get forwarded to an answering machine.

The IETF emergency services architecture addresses callbacks in a limited fashion and thereby covers a couple of scenarios. This document discusses some shortcomings and raises the question whether additional solution techniques are needed.

Table of Contents

1. Introduction

Summoning police, the fire department or an ambulance in emergencies is one of the fundamental and most-valued functions of the telephone. As telephone functionality moves from circuit-switched telephony to Internet telephony, its users rightfully expect that this core functionality will continue to work at least as well as it has for the legacy technology. New devices and services are being made available that could be used to make a request for help, which are not traditional telephones, and users are increasingly expecting them to be used to place emergency calls.

Regulatory requirements demand that the emergency call itself provides enough information to allow the call-taker to initiate a call back to the emergency caller in case the call dropped or to interact with the emergency caller in case of further questions. Such a call, referred as PSAP callback subsequently in this document, may, however, be blocked or forwarded to an answering machine as SIP entities (SIP proxies as well as the SIP UA itself) cannot associate the potential importantance of the call based on the SIP signaling.

> Note that the authors are, however, not aware of regulatory requirements for providing preferential treatment of callbacks initiated by the call-taker at the PSAP towards the emergency caller.

Section 10 of [I-D.ietf-ecrit-framework] discusses the identifiers required for callbacks, namely AOR URI and a globally routable URI in a Contact: header. Section 13 of [I-D.ietf-ecrit-framework] provides

the following guidance regarding callback handling:

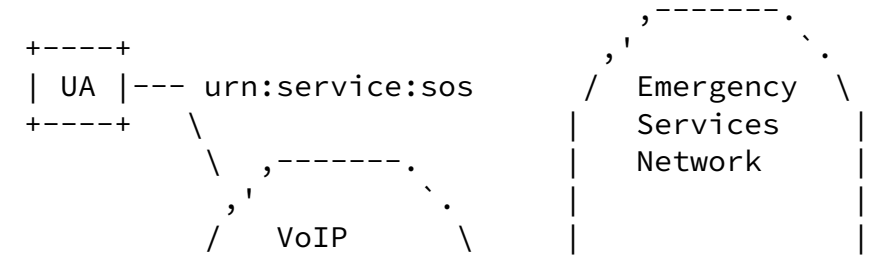
> A UA may be able to determine a PSAP call back by examining the domain of incoming calls after placing an emergency call and comparing that to the domain of the answering PSAP from the emergency call. Any call from the same domain and directed to the supplied Contact header or AoR after an emergency call should be accepted as a call-back from the PSAP if it occurs within a reasonable time after an emergency call was placed.

This approach mimics a stateful packet filtering firewall and is indeed helpful in a number of cases. Below, we discuss a few cases where this approach fails.

1.1. Multi-Stage Resolution

Consider the following emergency call routing scenario shown in Figure 1 where routing towards the PSAP occurs in several stages. An emergency call uses a SIP UA that does not run LoST on the end point.

Hence, the call is marked with the 'urn:service:sos' Service URN [RFC5031]. The user's VoIP provider receives the emergency call and determines where to route it. Local configuration or a LoST lookup might, in our example, reveal that emergency calls are routed via a dedicated provider FooBar and targeted to a specific entity, referred as esrp1@foobar.com. FooBar does not handle emergency calls itself but performs another resolution step to let calls enter the emergency services network and in this case another resolution step takes place and esrp-a@esinet.org is determined as the recipient, pointing to an edge device at the IP-based emergency services network. Inside the emergency services there might be more sophisticated routing taking place somewhat depending on the existing structure of the emergency services infrastructure.



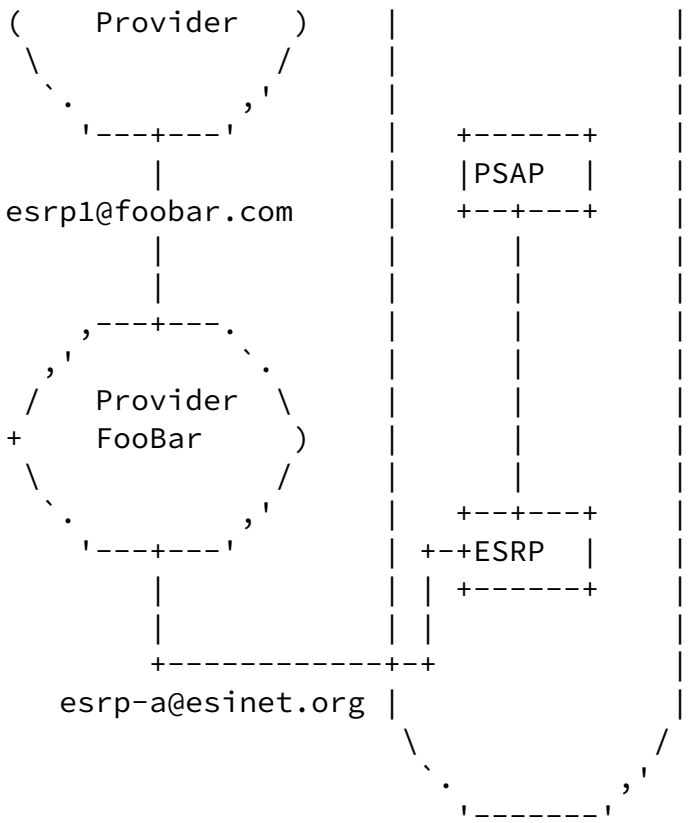
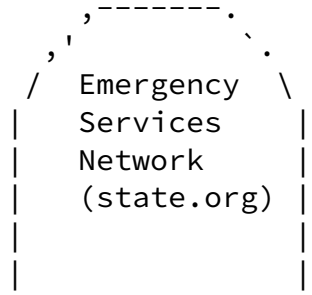


Figure 1: Multi-Stage Resolution

1.2. Call Forwarding

Imagine the following case where an emergency call enters an emergency network (state.org) via an ERSP but then gets forwarded to a different emergency services network (in our example to police-town.org, fire-town.org or medic-town.org). The same considerations apply when the the police, fire and ambulance networks are part of the state.org sub-domains (e.g., police.state.org).


Emergency
Services
Network
(state.org)

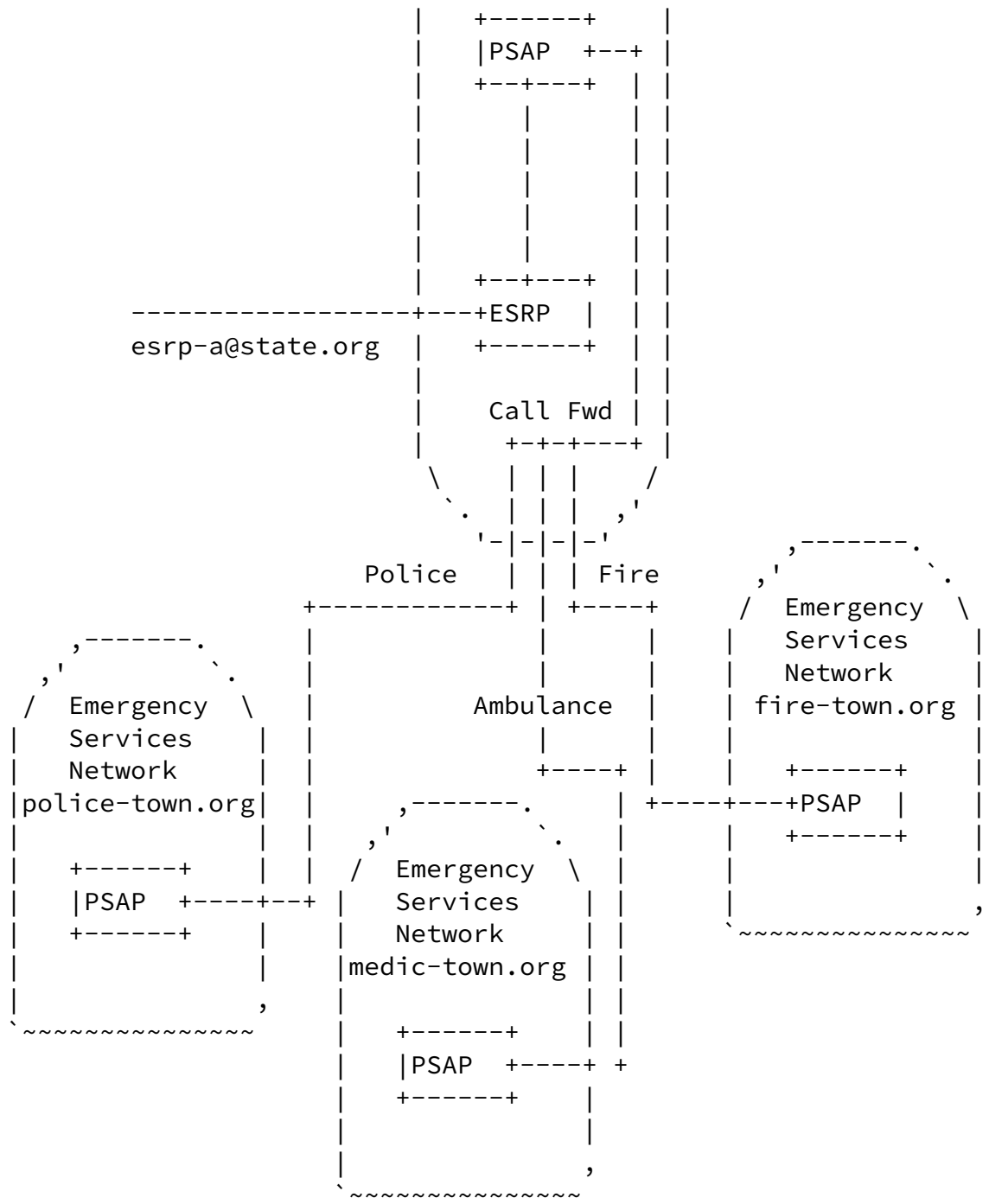


Figure 2: Call Forwarding

1.3. PSTN Interworking

In case an emergency call enters the PSTN, as shown in Figure 3, there is no guarantee that the callback some time later does leave the same PSTN/VoIP gateway or that the same end point identifier is used in the forward as well as in the backward direction making it difficult to reliably detect PSAP callbacks.

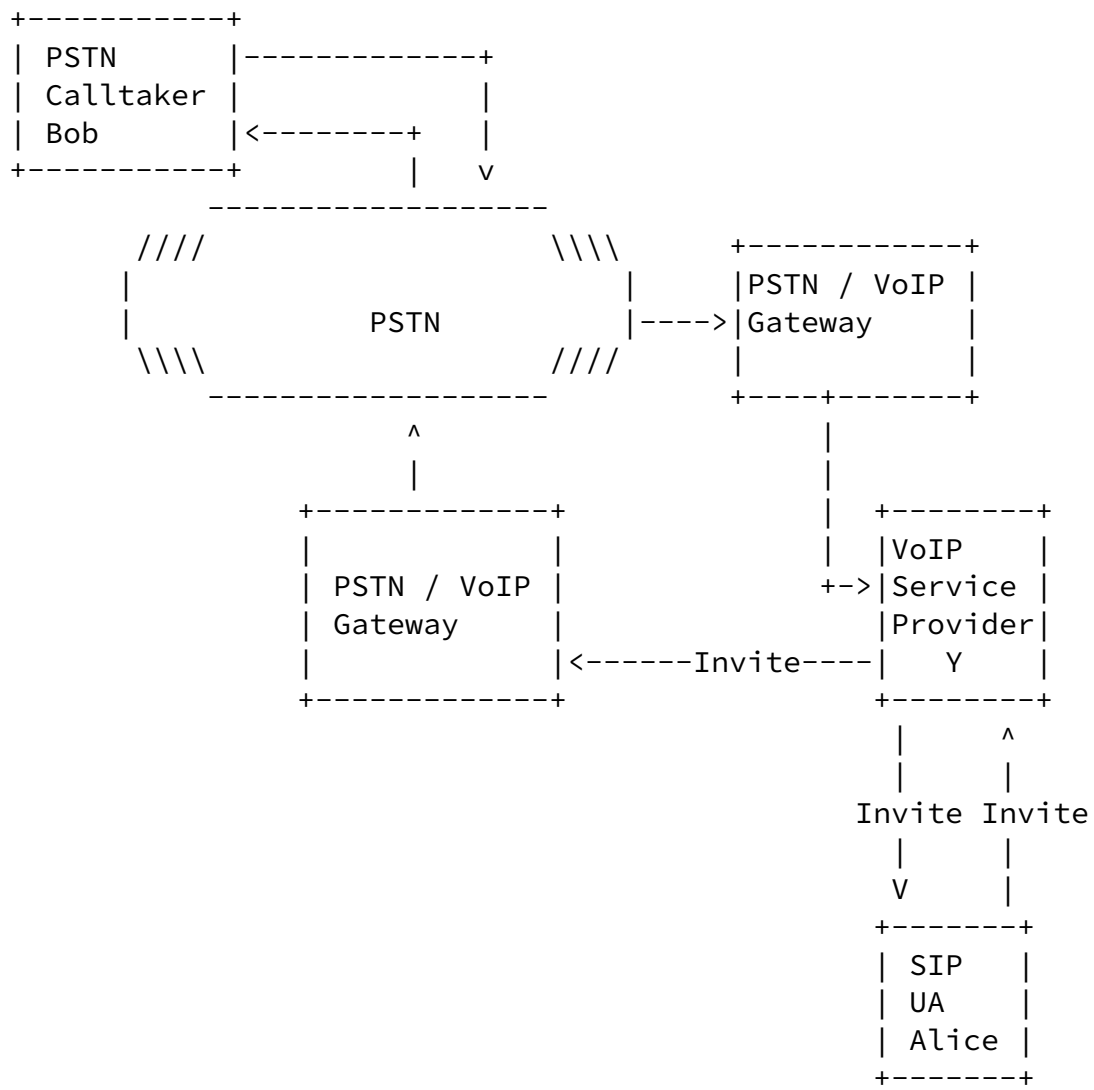


Figure 3: PSTN Interworking

2. Terminology

The key words "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].

Emergency services related terminology is borrowed from [RFC5012].

3. Requirements and Design Approaches

From the previously presented scenarios, the following generic requirements can be crafted:

Resistance Against Security Vulnerabilities:

The main possibility of attack involves use of the PSAP callback marking to bypass blacklists, ignore call forwarding procedures and similar features to interact with users and to raise their attention. For example, using PSAP callback marking devices would be able to recognize these types of incoming messages leading to the device overriding user interface configurations, such as vibrate-only mode. As such, the requirement is to ensure that the mechanisms described in this document can not be used for malicious purposes, including SPIT.

Fallback to Normal Call

When the newly defined extension is not recognized by intermediaries or other entities then it MUST NOT lead to a failure of the call handling procedure but rather a fall-back to a call that did not have any marking provided.

In addition to the high-level requirements there are a few design choices.

What is the granularity of the decision making?

There are a few choices that impact the solution mechanism quite considerably:

* Verify that the caller is a PSAP

* Verify that the call is in response to a previous emergency call.

* Verify that the call is related to an emergency, but not necessarily an earlier emergency call. This might include

public notification (authority-to-citizen).

Who calls back?

The relationship between the person who previously received the emergency call and the person who triggers the callback allows a couple of choices:

* The callback has to be made using the same User Agent.
* The callback has to made by the same user but potentially with a different UA.
* A different user from a different UA can make the callback.

4. Solution Approaches

This version of the document does not yet contain a fully specified solution description. Instead, it tries to explore the different alternatives.

An example solution can be found in an earlier version of [I-D.patel-ecrit-sos-parameter]. The "sos" URI parameter is appended to the URI in the Contact header field of the INVITE request for PSAP call-back establishment. Although this approach can distinguish the PSAP call-back from other sessions, such a solution is prone to security vulnerabilities since the insertion of the URI parameter cannot verify the request was generated from a PSAP rather than a malicious entity.

The usage of the In-Reply-To header field can provide the capability to relate the PSAP call-back to a previously made emergency call. The UA of the emergency caller, as well as enities within the service provider's network can therefore infer that the request is a PSAP callback, providing they maintained information pertaining to the emergency call. This solution also relies on the PSAP call-back routing over the same entities that the emergency call was routed over if such a solution is used to provide preferential treatment of callbacks. A solution based on the inclusion of the In-Reply-To header would be useful in the case the network or the UA is required

to disable services or features which may prevent the callback from reaching the UA from which the emergency call was placed. Furthermore, it may facilitate success of the callback by removing, for example, incoming call barring restrictions that may have been enforced for the emergency caller's service.

To fulfill the requirements of verifying the caller is a PSAP, mechanisms such as those described in RFC 4474 [RFC4474] or in RFC 3325 [RFC3325] are recommended to be used. Such an approach would mitigate security vulnerabilities, but does not explicitly mark the request generated from the PSAP as a request for callback. Additional information, such a PSAP whitelist, would have to be known. This is, however, only likely to work in a smaller scale rather than world wide.

The use of the Calling Party's Category URI parameter in the P-Asserted-Identity [RFC3325], as described in [I-D.patel-dispatch-cpc-oli-parameter], is one method of a network asserted identifier, describing the nature of the calling party and in this case, the PSAP. This approach only works when the entity that inserts the CPC parameter is trusted by those who verify it. This relies on a circle of trust similar to the a white list. Additionally, it has to be mentioned that unlike [I-D.ietf-sip-saml]

applying SIP Identity over the parameter does not ensure that the authentication service indeed asserts the validity of the parameter.

5. Security Considerations

This document provides discussions problems of PSAP callbacks and lists requirements, some of which illustrate security challenges. The current version does not yet provide a specific solution but rather starts with overall architectural observations.

An important aspect from a security point of view is the relationship between the emergency services network and the VSP (assuming that the emergency call travels via the VSP and not directly between the SIP UA and the PSAP). If there is a strong trust relationship between

the PSAP operator and the VSP (for example based on a peering relationship) without any intermediate VoIP providers then the identification of a PSAP call back is less problematic than in the case where the two entities have not entered in some form of relationship that would allow the VSP to verify whether the marked callback message indeed came from a legitimate source.

6. Acknowledgements

We would like to thank members from the ECRIT working group, in particular Brian Rosen, for their discussions around PSAP callbacks.

7. References

7.1. Informative References

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

7.2. Informative References

[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.

[I-D.ietf-sip-saml]
Tschofenig, H., Hodges, J., Peterson, J., Polk, J., and D. Sicker, "SIP SAML Profile and Binding", draft-ietf-sip-saml-06 (work in progress), March 2009.

[I-D.patel-dispatch-cpc-oli-parameter]
Patel, M., Jesske, R., and M. Dolly, "Uniform Resource Identifier (URI) Parameters for indicating the Calling Party's Catagory and Originating Line Identity", draft-patel-dispatch-cpc-oli-parameter-00 (work in progress), October 2009.

[I-D.patel-ecrit-sos-parameter]
Patel, M., "SOS Uniform Resource Identifier (URI) Parameter for Marking of Session Initiation Protocol (SIP) Requests related to Emergency Services", draft-patel-ecrit-sos-parameter-06 (work in progress), May 2009.

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC4474] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for

Emergency and Other Well-Known Services", RFC 5031, January 2008.

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

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

Milan Patel
Nortel
Maidenhead Office Park, Westacott Way
Maidenhead SL6 3QH
UK

Email: milanpa@nortel.com