ECRIT	H. Schulzrinne
Internet-Draft	Columbia University
Intended status: Standards Track	H. Tschofenig
Expires: April 29, 2012	Nokia Siemens Networks
	C.H. Holmberg
	Ericsson
	M. Patel
	InterDigital Communications
	October 27, 2011

Public Safety Answering Point (PSAP) Callback
draft-ietf-ecrit-psap-callback-03.txt

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. 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, 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 offers capabilities to allow callbask to bypass authorization policies to reach the caller without unnecessary delays. However, the mechanism specified prior to this document supports only limited scenarios. This document discusses some shortcomings, presents additional scenarios where better-than-normal call treatment behavior would be desirable, and specifies a protocol solution.

Status of this Memo

Copyright Notice

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.

An overview of the protocol interactions for emergency calling using the IETF emergency services architecture are described in [I-D.ietf-ecrit-framework] and [I-D.ietf-ecrit-phonebcp] specifies the technical details. As part of the emergency call setup procedure two important identifiers are conveyed to the PSAP call-taker's user agent, namely the Address-Of-Record (AoR), and the Globally Routable User Agent (UA) URIs (GRUU). RFC 3261 [RFC3261] defines the AoR as: [RFC5627] specifies how to obtain and use GRUUs.

- An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

In SIP systems a single user can have a number of user agents (handsets, softphones, voicemail accounts, etc.) which are all referenced by the same AOR. There are a number of cases in which it is desirable to have an identifier which addresses a single user agent rather than the group of user agents indicated by an AOR. The GRUU is such a unique user- agent identifier, which is still globally routable. 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. The AoR and the GRUU serve this purpose. The communication attempt by the PSAP call-taker back to the emergency caller is called 'PSAP callback'.

A PSAP callback may, however, be blocked by user configured whitelis or may be forwarded to an answering machine as SIP entities (SIP proxies as well as the SIP UA itself) cannot differentiate the callback from any other SIP call establishing attempt from the SIP signaling message. While there are no regulatory requirements at the time of writing of this specification there is the believe that PSAP callbacks have to be treated in such a way that they reach the emergency caller. For this purpose guidance for PSAP callback handling has been provided in Section 13 of [I-D.ietf-ecrit-framework]:

- 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 callback 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. It is also relatively simple to implement. Unfortunately, it does not work in all SIP deployment scenarios. In Section 3 we describe scenarios where the currently standardized approach is insufficient. In Section 4 a solution is described.

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. Callback Scenarios

This section illustrates a number of scenarios where the currently specified solution, as specified in [I-D.ietf-ecrit-phonebcp], for preferential treatment of callbacks fails. As explained in Section 1 a SIP entity examines an incoming PSAP call back by comparing the domain of the PSAP with the destination domain of the emergency call.

3.1. Routing Asymmetry

In some deployment environments it is common to have incoming and outgoing SIP messaging routed through different SIP entities. Figure 1 shows this graphically whereby a VoIP provider uses different SIP proxies for inbound and for outbound call handling. Unless they two devices are state synchronized the callback hitting the inbound proxy would get treated like any other call since the emergency call established state information at the outbound proxy only.

```
                                                ,-------.
                                              ,'         `.
                   ,-------.                 /  Emergency  \
                 ,'         `.              |   Services    |
                /  VoIP       \      I      |   Network     |
               |   Provider    |     n      |               |
               |               |     t      |               |
               |               |     e      |               |
               |   +-------+   |     r      |               |
            +--+---|Inbound|<--+-----m      |               |
            |  |   |Proxy  |   |     e      |   +------+    |
            |  |   +-------+   |     d      |   |PSAP  |    |
            |  |               |     i      |   +--+---+    |
  +----+    |  |               |     a-+    |      |        |
  | UA |<---+  |               |     t |    |      |        |
  |    |----+  |               |     e |    |      |        |
  +----+    |  |               |       |    |      |        |
            |  |               |     P  |   |      |        |
            |  |               |     r  |   |      |        |
            |  |   +--------+  |     o   |  |      |        |
            +--+-->|Outbound|--+---->v   |  |   +--+---+    |
               |   |Proxy   |  |     i    | | +-+ESRP  |    |
               |   +--------+  |     d    | | | +------+    |
               |               |     e     || |             |
               |               |     r     |+-+             |
                \             /             |               |
                 `.         ,'               \             /
                   '-------'                  `.         ,'
                                                '-------'
```

3.2. Multi-Stage Routing

Consider the following emergency call routing scenario shown in Figure 2 where routing towards the PSAP occurs in several stages. In this scenario we consider a SIP UA that uses LoST to learn the next hop destination closer to the PSAP. This call is then sent to the user's VoIP provider. The user's VoIP provider receives the emergency call and creates state based on the destination domain, namely state.com. It then routes it to the indicated ESRP. When the ESRP receives it it needs to decide what the next hop is to get it closer to the PSAP. In our example the next hop is the PSAP with the URI psap@town.com. When a callback is sent from psap@town.com towards the emergency caller the call will get normal treatment by the VoIP providers inbound proxy since the domain of the PSAP does not match the stored state information.

```
                                      ,-------.
    +----+                          ,'         `.
    | UA |--- esrp1@foobar.com     /  Emergency  \
    +----+   \                    |   Services    |
              \  ,-------.        |   Network     |
               ,'         `.      |               |
              /   VoIP      \     |   +------+    |
             (    Provider   )    |   |PSAP  |    |
              \             /     |   +--+---+    |
               `.         ,'      |      |
                 '---+---'        |      |        |
                     |            |psap@town.com  |
             esrp@state.com       |      |        |
                     |            |      |        |
                     |            |      |        |
                     |            |   +--+---+    |
                     +------------+---+ESRP  |    |
                                  |   +------+    |
                                  |               |
                                   \             /
                                    `.         ,'
                                      '-------'
```

3.3. 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).

Similarly to the previous scenario the problem here is with the wrong state information being established during the emergency call setup procedure. A callback would originate in the police-town.org, fire-town.org or medic-town.org domain whereas the emergency caller's SIP UA or the VoIP outbound proxy has stored state.org.

```
                              ,-------.
                            ,'         `.
                           /  Emergency  \
                          |   Services    |
                          |   Network     |
                          |   (state.org) |
                          |               |
                          |               |
                          |   +------+    |
                          |   |PSAP  +--+ |
                          |   +--+---+  | |
                          |      |      | |
                          |      |      | |
                          |      |      | |
                          |      |      | |
                          |      |      | |
                          |   +--+---+  | |
        ------------------+---+ESRP  |  | |
        esrp-a@state.org  |   +------+  | |
                          |             | |
                          |    Call Fwd | |
                          |     +-+-+---+ |
                           \    | | |    /
                            `.  | | |  ,'
                              '-|-|-|-'           ,-------.
                       Police   | | | Fire      ,'         `.
                   +------------+ | +----+     /  Emergency  \
    ,-------.      |              |      |    |   Services    |
  ,'         `.    |              |      |    |   Network     |
 /  Emergency  \   |          Ambulance  |    | fire-town.org |
|   Services    |  |              |      |    |               |
|   Network     |  |              +----+ |    |   +------+    |
|police-town.org|  |     ,-------.     | +----+---+PSAP  |    |
|               |  |   ,'         `.   |      |   +------+    |
|   +------+    |  |  /  Emergency  \  |      |               |
|   |PSAP  +----+--+ |   Services    | |      |               ,
|   +------+    |    |   Network     | |      `~~~~~~~~~~~~~~~
|               |    |medic-town.org | |
|               ,    |               | |
`~~~~~~~~~~~~~~~     |   +------+    | |
                     |   |PSAP  +----+ +
                     |   +------+    |
                     |               |
                     |               ,
                     `~~~~~~~~~~~~~~~
```

3.4. Network-based Service URN Resolution

The IETF emergency services architecture also considers cases where the resolution from the Service URN to the PSAP URI does not only happen at the SIP UA itself but at intermediate SIP entities, such as the user's VoIP provider.
Figure 4 shows this message exchange of the outgoing emergency call and the incoming PSAP graphically. While the state information stored at the VoIP provider is correct the state allocated at the SIP UA is not.

```
     ,-------.
   ,'         `.
  /  Emergency  \
 |   Services    |
 |   Network     |
 |police-town.org|
 |               |
 |   +------+    |    Invite to police.example.com
 |   |PSAP  +<---+------------------------+
 |   |      +----+------------------+     ^
 |   +------+    |Invite from       |     |
 |               ,police.example.com|     |
 `~~~~~~~~~~~~~~~                   v     |
 +--------+                        ++-----+-+
 |        |            query       |VoIP    |
 | LoST   |<-----------------------|Service |
 | Server |   police.example.com   |Provider|
 |        |----------------------->|        |
 +--------+                        +--------+
                                    |     ^
                              Invite|     | Invite
                                from|     | to
                  police.example.com|     | urn:service:sos
                                    V     |
                                   +-------+
                                   | SIP   |
                                   | UA    |
                                   | Alice |
                                   +-------+
```

3.5. PSTN Interworking

In case an emergency call enters the PSTN, as shown in Figure 5, 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.

```
  +-----------+
  | PSTN      |-------------+
  | Calltaker |             |
  | Bob       |<--------+   |
  +-----------+         |   v
             -------------------
         ////                   \\\\      +------------+
        |                           |     |PSTN / VoIP |
        |             PSTN          |---->|Gateway     |
         \\\\                   ////      |            |
             -------------------          +----+-------+
                        ^                      |
                        |                      |
                  +-------------+              |  +--------+
                  |             |              |  |VoIP    |
                  | PSTN / VoIP |              +->|Service |
                  | Gateway     |                 |Provider|
                  |             |<------Invite----|   Y    |
                  +-------------+                 +--------+
                                                   |     ^
                                                   |     |
                                                 Invite Invite
                                                   |     |
                                                   V     |
                                                  +-------+
                                                  | SIP   |
                                                  | UA    |
                                                  | Alice |
                                                  +-------+
```

Note: This scenario is considered outside the scope of this document. The specified solution does not support this use case.

4. Specification

[Editor's Note: The solution approach described in [I-D.holmberg-emergency-callback-id] will be discussed at the IETF#82 ECRIT meeting and at the ECRIT mailing list and will be incorporated here if agreed by the working group.]

5. Security Considerations

[Editor's Note: Instead of an abstract security description text will be provided with the solution description.]

6. IANA Considerations

[Editor's Note: IANA consideration text will be added once an agreement on the solution has been reached.

7. Acknowledgements

We would like to thank members from the ECRIT working group, in particular Brian Rosen, for their discussions around PSAP callbacks. The working group discussed the topic of callbacks at their virtual interim meeting in February 2010 and the following persons provided valuable input: John Elwell, Bernard Aboba, Cullen Jennings, Keith Drage, Marc Linsner, Roger Marshall, Dan Romascanu, Geoff Thompson, Janet Gunn.
At IETF#81 a small group of people got to together to continue the discussions started at the working group meeting to explore a GRUU-based solution approach. Martin Thomson, Marc Linsner, Andrew Allen, Brian Rosen, Martin Dolly, and Atle Monrad participated at this side-meeting.
Finally, we would like to thank Cullen Jennings for his discussion input. He was the first to propose a "token-based" solution.

8. References

8.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
[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.
[RFC3966]	Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.
[RFC3969]	Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)", BCP 99, RFC 3969, December 2004.
[RFC5627]	Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.
[RFC5341]	Jennings, C and V. K. Gurbani, "The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry", September 2008.
[RFC4474]	Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

8.2. Informative References

[I-D.ietf-ecrit-framework]	Rosen, B, Schulzrinne, H, Polk, J and A Newton, "Framework for Emergency Calling using Internet Multimedia", Internet-Draft draft-ietf-ecrit-framework-13, September 2011.
[I-D.ietf-ecrit-phonebcp]	Rosen, B and J Polk, "Best Current Practice for Communications Services in support of Emergency Calling", Internet-Draft draft-ietf-ecrit-phonebcp-20, September 2011.
[I-D.ietf-sip-saml]	Tschofenig, H, Hodges, J, Peterson, J, Polk, J and D Sicker, "SIP SAML Profile and Binding", Internet-Draft draft-ietf-sip-saml-08, October 2010.
[I-D.holmberg-emergency-callback-id]	Holmberg, C, "Session Initiation Protocol (SIP) emergency call back identification", Internet-Draft draft-holmberg-emergency-callback-id-00, October 2011.
[RFC4484]	Peterson, J., Polk, J., Sicker, D. and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)", RFC 4484, 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.
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

Appendix A. Alternative Solutions Considered

In an attempt to describe the problem and to explore solution approaches the working group had also investigated alternative approaches. We document them here for completeness. The solutions fall into three categories: (1) Identity-based authorization, (2) Trait-based authorization, and (3) Call Marking. Even though these solutions are not mutually exclusive we describe them in separate sub-sections. Beyond the disadvantages listed in each solution category none of them provides the emergency caller with the ability to restrict preferential PSAP callback handling to those cases where an earlier emergency call was initiated.

Appendix A.1. Identity-based Authorization

In Figure 6 an interaction is presented that allows a SIP entity to make a policy decision whether to bypass installed authorization policies and thereby providing preferential treatment. To make this decision the sender's identity is compared with a whitelist of valid PSAPs. The identity assurances in SIP can come in different forms, such as SIP Identity [RFC4474] or with P-Asserted-Identity [RFC3325]. The former technique relies on a cryptographic assurance and the latter on a chain of trust.

```
                 +----------+
                 | List of  |+
                 | valid    ||
                 | PSAP ids ||
                 +----------+|
                  +----------+
                      *
                      * whitelist
                      *
                      V
   Incoming      +----------+    Normal
   SIP Msg       | SIP      |+   Treatment
  -------------->| Entity   ||=============>
   + Identity    |          ||(if not in whitelist)
                 +----------+|
                 +----------+
                      ||
                      ||
                      || Preferential
                      || Treatment
                      ++=============>
                        (in whitelist)
```

This approach was not chosen because the establishment of a whitelist containing PSAP identities is operationally complex and does not easily scale world wide. Only when there is a local relationship between the VSP/ASP and the PSAP then populating the whitelist is far simpler. This would, however, constrain the applicability of the mechanism considerably.

Appendix A.2. Trait-based Authorization

An alternative approach to an identity based authorization model is outlined in Figure 7. In fact, RFC 4484 [RFC4484] illustrates a related emergency service use case.

```
               +----------+
               | List of  |+
               | trust    ||
               | anchor   ||
               +----------+|
                +----------+
                    *
                    *
                    *
                    V
 Incoming      +----------+    Normal
 SIP Msg       | SIP      |+   Treatment
-------------->| Entity   ||=============>
 + trait       |          ||(no indication
               +----------+| of PSAP)
               +----------+
                    ||
                    ||
                    || Preferential
                    || Treatment
                    ++=============>
                      (indicated as
                       PSAP)
```

In a trait-based authorization scenario an incoming SIP message contains a form of trait, i.e. some form of assertion. The assertion contains an indication that the sending party has the role of a PSAP (or similar emergency services entity). The assertion is either cryptographically protected to enable end-to-end verification or an chain of trust security model has to be assumed. In Figure 7 we assume an end-to-end security model where trust anchors are provisioned to ensure the ability for a SIP entity to verify the received assertion. This solution was not chosen because trait-based authorization never got deployed in SIP. Furthermore, in order to ensure that the assertions are properly protected it is necessary to digitally sign, which requires some form of public key infrastructure for usage with emergency services. Finally, there need to be some policies in place that define which entities are allowed to obtain various roles. These policies and procedures do not exist today.

Appendix A.3. Call Marking

Call marking allows the PSAP to place a non-cryptographic label on outgoing calls that gives, when received by a SIP entity, preferential treatment for these callbacks.
When used in isolation this mechanism introduces considerable denial of service attacks due to the ability to bypass any authorization policies and could be utilized to distribute unwanted traffic.

Authors' Addresses

Henning Schulzrinne 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 Tschofenig Nokia Siemens Networks Linnoitustie 6 Espoo, 02600 Finland Phone: +358 (50) 4871445 EMail: Hannes.Tschofenig@gmx.net URI: http://www.tschofenig.priv.at

Christer Holmberg Holmberg Ericsson Hirsalantie 11 Jorvas, 02420 Finland EMail: christer.holmberg@ericsson.com

Milan Patel Patel InterDigital Communications EMail: Milan.Patel@interdigital.com