ECRIT
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2014

H. Schulzrinne
Columbia University
H. Tschofenig
Nokia Siemens Networks
C. Holmberg
Ericsson
M. Patel
InterDigital Communications

July 13, 2013

Public Safety Answering Point (PSAP) Callback
draft-ietf-ecrit-psap-callback-10.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 specification already offers a solution approach for allowing PSAP callbacks to bypass authorization policies to reach the caller without unnecessary delays. Unfortunately, the specified mechanism only supports limited scenarios. This document discusses shortcomings of the current mechanisms and illustrates additional scenarios where better-than-normal call treatment behavior would be desirable. A solution based on a new header field value, called "psap-callback", for the SIP Priority header field is specified to accomplish the PSAP callback marking.

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 [RFC6443] and [RFC6881] 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, if available, the Globally Routable User Agent (UA) URIs (GRUU). RFC 3261 [RFC3261] defines the AOR as:

> "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. RFC 5627 [RFC5627] specifies how to obtain and use GRUUs. [RFC6881] also makes use of the GRUU for emergency calls.

Regulatory requirements demand that the emergency call setup procedure itself provides enough information to allow the call taker to initiate a callback to the emergency caller. This is desirable in those cases where the call got dropped prematurely or when further communication need arises. 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 authorization policies or may be forwarded to an answering machine since SIP entities (SIP proxies as well as the SIP user equipment itself) cannot differentiate the PSAP callback from any other SIP call. "Call barring", "do not disturb", or "call diversion"(aka call forwarding) are features that prevent delivery of a call. It is important to note that these features may be implemented by SIP intermediaries as well as by the user agent.

Among the emergency services community there is the desire to offer PSAP callbacks a treatment such that chances are increased that it reaches the emergency caller. At the same time a design must deal with the negative side-effects of allowing certain calls to bypass call forwarding or other authorization policies. Ideally, the PSAP callback has to relate to an earlier emergency call that was made "not too long ago". An exact time interval is difficult to define in a global IETF standard due to the variety of national regulatory requirements.

To nevertheless meet the needs from the emergency services community a basic mechanism for preferential treatment of PSAP callbacks was defined in Section 13 of [RFC6443]. The specification says:

> "A UA may be able to determine a PSAP callback 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 even though it requires call state to be maintained by the user agent as well as by SIP intermediaries. Unfortunately, the solution does not work in all deployment scenarios. In Section 3 we describe cases where the currently standardized approach is insufficient.

2. Terminology

Emergency services related terminology is borrowed from [RFC5012]. This includes terminology like emergency caller, user equipment, call taker, Emergency Service Routing Proxy (ESRP), and Public Safety Answering Point (PSAP).

3. Callback Scenarios

This section illustrates a number of scenarios where the currently specified solution, as specified in [RFC6881], for preferential treatment of callbacks fails. As explained in Section 1 a SIP entity examines an incoming PSAP callback by comparing the domain of the PSAP with the destination domain of the emergency call.

NOTE: All FQDNs used in the subsections below are used for illustrative purposes. They are examples to demonstrate the limitations of the technical solution outlined in RFC 6881.

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 the two devices are synchronized as to state 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     |+-+             |
                   \             /             |               |
```

```
                    `.         ,'                \             /
                      '-------'                   `.        ,'
                                                    '-------'
```

Figure 1: Example for Routing Asymmetry.

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.org. 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.org       |      |        |
                        |            |      |        |
                        |            |      |        |
                        |            |   +--+----+   |
                        +------------+----+ESRP  |   |
                                     |   +-------+   |
                                     |               |
                                      \             /
                                       `.         ,'
                                         '-------'
```

Figure 2: Example for Multi-Stage Routing.

3.3. Call Forwarding

Imagine the following case where an emergency call enters an emergency network (state.org) via an ESRP 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 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  +----+ +
                        |   +------+    |
                        |               |
                        |               ,
                        `~~~~~~~~~~~~~~~
```

Figure 3: Example for Call Forwarding.

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 |
                                     +-------+
```

Figure 4: Example for Network-based Service URN Resolution.

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 |
                                                   +-------+
```

Figure 5: Example for PSTN Interworking.

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

4. SIP PSAP Callback Indicator

4.1. General

This section defines a new header field value, called "psap-callback", for the SIP Priority header field defined in [RFC3261]. The value is used to inform SIP entities that the request is associated with a PSAP callback SIP session.

4.2. Usage

SIP entities that receive the header field value within an initial request for a SIP session can, depending on local policies, apply PSAP callback specific procedures for the session or request.

The PSAP callback specific procedures may be applied by SIP-based network entities and by the callee. The specific procedures taken when receiving such a PSAP callback marked call, such as bypassing services and barring procedures, are outside the scope of this document.

4.3. Syntax

4.3.1. General

This section defines the ABNF for the new SIP Priority header field value "psap-callback".

4.3.2. ABNF

```
priority-value  /=  "psap-callback"
```

Figure 6: ABNF

5. Security Considerations

5.1. Security Threat

The PSAP callback functionality described in this document allows marked calls to bypass blacklists, ignore call forwarding procedures and other similar features used to raise the attention of emergency callers when attempting to contact them. In the case where the SIP Priority header value, 'psap-callback', is supported by the SIP UA, it would override user interface configurations, such as vibrate-only mode, to alert the caller of the incoming call.

5.2. Security Requirements

The requirement is to ensure that the mechanisms described in this document can not be used for malicious purposes, including telemarketing.

Furthermore, if the newly defined extension is not recognized, not verified adequately, or not obeyed by SIP intermediaries or SIP endpoints then it must not lead to a failure of the call handling procedure. Such call must be treated like a call that does not have any marking attached.

5.3. Security Solution

Figure 7 shows the architecture that utilizes the identity of the PSAP to decide whether a preferential treatment of callbacks should be provided. To make this policy decision, the identity of the PSAP is compared with a white list of valid PSAPs available to the SIP entity. The identity assurance 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. Also the usage of TLS between neighboring SIP entities may provide useful identity information.

```
                  +----------+
                  | List of  |+
                  | valid    ||
                  | PSAPs    ||
                  +----------+|
                   +----------+
                       *
                       * white list
                       *
                       V
    Incoming      +----------+    Normal
    SIP Msg       | SIP      |+   Treatment
   -------------->| Entity   ||=====================>
    + Identity    |          ||(if not in white list)
      Info        +----------+|
                  +----------+
                       ||
                       ||
                       || Preferential
                       || Treatment
                       ++========================>
                         (if successfully verified)
```

Figure 7: Identity-based Authorization

An important aspect from a security point of view is the relationship between the emergency services network (containing PSAPs) and the VoIP provider (assuming that the emergency call travels via the VoIP provider and not directly between the SIP UA and the PSAP).

If there is some form of relationship between the emergency services operator and the VoIP provider then the identification of a PSAP callback is less problematic than in the case where the two entities have not entered in some form of relationship that would allow the VoIP provider to verify whether the marked callback message indeed came from a legitimate source.

The establishment of a whitelist with PSAP identities maybe be operationally complex. When there is a local relationship between the VoIP provider and the PSAP then populating the whitelist is fairly simple. For SIP UAs there is no need to maintain a list of PSAPs. Instead SIP UAs are assumed to trust the correct processing of their VoIP provider, i.e., the VoIP provider processes the PSAP callback marking and, if it cannot be verified, the PSAP callback marking is removed. If it is left untouched then the SIP UA should assume that it has been verified successfully by the VoIP provider and it should therefore be obeyed.

6. IANA Considerations

This document adds the "psap-callback" value to the SIP Priority header IANA registry allocated by [RFC6878]. The semantic of the newly defined "psap-callback" value is defined in Section 4.

7. Acknowledgements

We would like to thank the following persons for their feedback: Paul Kyzivat, Martin Thomson, Robert Sparks, Keith Drage, Cullen Jennings Brian Rosen, Martin Dolly, Bernard Aboba, Andrew Allen, Atle Monrad, John-Luc Bakker, John Elwell, Geoff Thompson, Dan Romascanu, James Polk, John Medland, Hadriel Kaplan, Kenneth Carlberg, Timothy Dwight, Janet Gunn

Finally, we would like to thank the ECRIT working group chairs, Marc Linsner and Roger Marshall, for their support. Roger Marshall was the document shepherd for this document.

8. References

8.1. Normative References

[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.

[RFC5627] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.

[RFC6878] Roach, A., "IANA Registry for the Session Initiation Protocol (SIP) "Priority" Header Field", RFC 6878, March 2013.

8.2. Informative References

[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.

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

[RFC6881] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling", BCP 181, RFC 6881, March 2013.

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

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: christer.holmberg@ericsson.com

Milan Patel
InterDigital Communications

EMail: Milan.Patel@interdigital.com