ECRIT	H. Schulzrinne
Internet-Draft	Columbia University
Intended status: Informational	H. Tschofenig
Expires: April 28, 2011	Nokia Siemens Networks
	M. Patel
	Nortel
	October 25, 2010

Public Safety Answering Point (PSAP) Callbacks
draft-ietf-ecrit-psap-callback-01.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 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 illustrates an extension.

Status of this Memo

Copyright Notice

Table of Contents

---

1. Introduction

TOC

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] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2010.) 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] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2010.) 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. It is also relatively simple to implement. Below, we discuss a few cases where this approach fails.

1.1. Routing Asymmetry

TOC

In some deployment environments it is common to have incoming and outgoing SIP messaging to use different routes.

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

1.2. Multi-Stage Resolution

TOC

Consider the following emergency call routing scenario shown in Figure 2 (Example for Multi-Stage Resolution) 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] (Schulzrinne, H., “A Uniform Resource Name (URN) for Emergency and Other Well-Known Services,” January 2008.). 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.

```
                                        ,-------.
      +----+                          ,'         `.
      | UA |--- urn:service:sos      /  Emergency  \
      +----+   \                    |   Services    |
                \  ,-------.        |   Network     |
                 ,'         `.      |               |
                /   VoIP      \     |               |
               (    Provider   )    |               |
                \             /     |               |
                 `.         ,'      |               |
                   '---+---'        |   +------+    |
                       |            |   |PSAP  |    |
               esrp1@foobar.com     |   +--+---+    |
                       |            |      |        |
                       |            |      |        |
                   ,---+---.        |      |        |
                 ,'         `.      |      |        |
                /   Provider  \     |      |        |
               +    FooBar     )    |      |        |
                \             /     |      |        |
                 `.         ,'      |   +--+---+    |
                   '---+---'        | +-+ESRP  |    |
                       |            | | +------+    |
                       |            | |             |
                       +------------+-+             |
                  esrp-a@esinet.org |               |
                                     \             /
                                      `.         ,'
                                        '-------'
```

Figure 2: Example for Multi-Stage Resolution

1.3. Call Forwarding

TOC

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) |
                          |               |
                          |               |
                          |   +------+    |
                          |   |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

1.4. PSTN Interworking

TOC

In case an emergency call enters the PSTN, as shown in Figure 4 (Example for PSTN Interworking), 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 4: Example for PSTN Interworking

1.5. Network-based Service URN Resolution

TOC

The mechanism described in [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2010.) assumes that all devices at the call signaling path store information about the domain of the communication recipient. This is necessary to match the stored domain name against the domain of the sender when an incoming call arrives.

However, the IETF emergency services architecture also considers those cases where the resolution from the Service URN to the PSAP URI happens somewhere in the network rather than immediately at the end point itself. In such a case, the end device is therefore not able to match the domain of the sender with any information from the outgoing emergency call.

Figure 5 (Example for Network-based Service URN Resolution) shows this message exchange graphically.

```
       ,-------.
     ,'         `.
    /  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 5: Example for Network-based Service URN Resolution

---

2. Terminology

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

Emergency services related terminology is borrowed from [RFC5012] (Schulzrinne, H. and R. Marshall, “Requirements for Emergency Context Resolution with Internet Technologies,” January 2008.).

3. Architecture

TOC

Section 4 (Callback Marking) describes how to mark a call as a callback. However, the pure emergency service callback marking is insufficient since it lacks any built-in security mechanism. Fortunately, available SIP security techniques for the purpose of authorization can be re-used, as described in the rest of the section. In Figure 6 (Identity-based Authorization) 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] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.) or with P-Asserted-Identity [RFC3325] (Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.). 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)
```

Figure 6: Identity-based Authorization

The establishment of a whitelist with PSAP identities is operationally complex and does not easily scale world wide. When there is a local relationship between the VSP/ASP and the PSAP then populating the whitelist is far simpler.
An alternative approach to an identity based authorization model is outlined in Figure 7 (Trait-based Authorization). In fact, RFC 4484 [RFC4484] (Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)," August 2006.) already illustrated the basic requirements for this technique.

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

Figure 7: Trait-based Authorization

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 (Trait-based Authorization) 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.

---

4. Callback Marking

TOC

The callback marking is represented as URI parameter for an URI scheme. The ABNF [RFC5234] (Crocker, D. and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” January 2008.) syntax is as follows. The 'par' production is defined in RFC 3966 [RFC3966] (Schulzrinne, H., “The tel URI for Telephone Numbers,” December 2004.). The "/=" syntax indicates an extension of the production on the left-hand side:

```
par /= callback
callback = callback-tag "=" callback-value
callback-tag = "callback"
callback-value = "normal" / "test" /
```

The semantics of the callback values are described below:
normal: This represents an normal PSAP callback.
test: This is a test callback.
An example of the "callback" parameter is given below:

```
From: <tel:+17005554141;callback=test>;tag=1928301774
```

---

5. Security Considerations

TOC

This document defines a callback marking scheme using URI parameters and illustrates how to handle authorization for preferential treatment. 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 some form of relationship between the emergency services operator and the VSP 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.
The main attack surface can be seen in the usage of PSAP callback marking to bypass blacklists, ignore call forwarding procedures and similar features to interact with users and to get 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.

It is important that PSAP callback marked SIP messages, which cannot be verified adequately, are treated like a call that does not have any marking attached instead of failing the call processing procedure.

6. IANA Considerations

TOC

This document extends the registry of URI parameters, as defined RFC 3969 [RFC3969] (Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)," December 2004.). Two new URI parameters are defined in this document as follows:
Parameter Name: callback
Predefined Values: Yes
Reference: This document

7. Acknowledgements

TOC

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, Milan Patel, Janet Gunn.

8. References

TOC

8.1. Informative References

TOC

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

8.2. Informative References

TOC

Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet

[I-D.ietf-ecrit-framework]	Multimedia," draft-ietf-ecrit-framework-11 (work in progress), July 2010 (TXT).
[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-08 (work in progress), October 2010 (TXT).
[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 (TXT).
[RFC3966]	Schulzrinne, H., "The tel URI for Telephone Numbers," RFC 3966, December 2004 (TXT).
[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 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," RFC 4474, August 2006 (TXT).
[RFC4484]	Peterson, J., Polk, J., Sicker, D., and H. Tschofenig, "Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)," RFC 4484, August 2006 (TXT).
[RFC5012]	Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies," RFC 5012, January 2008 (TXT).
[RFC5031]	Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services," RFC 5031, January 2008 (TXT).
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," STD 68, RFC 5234, January 2008 (TXT).

Authors' Addresses

TOC

	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