ecrit B. Rosen
Internet-Draft NeuStar
Intended status: Standards Track J. Polk
Expires: September 6, 2007 Cisco Systems
March 05, 2007

Best Current Practice for Communications Services in support of Emergency Calling
draft-ietf-ecrit-phonebcp-01.txt

Status of this Memo

Copyright Notice

Abstract

Requesting help in an emergency using a communications device such as a telephone or mobile is an accepted practice in most of the world. As communications devices increasingly utilize the Internet to interconnect and communicate, users will continue to expect to use such devices to request help, regardless of whether or not they communicate using IP. The emergency response community will have to upgrade their facilities to support the wider range of communications services, but cannot be expected to handle wide variation in device and service capability. The IETF has several efforts targeted at standardizing various aspects of placing emergency calls. This memo describes best current practice on how devices and services should use such standards to reliably make emergency calls

Table of Contents

1. Requirements notation

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].

2. Introduction

This document describes how SIP User Agents and proxy servers support emergency calling, as outlined in [I-D.ietf-ecrit-framework]. Here, an emergency call refers to a communications session established by a user to a "Public Safety Answering Point" (PSAP) which is a call center established by response agencies to accept emergency calls. We differentiate such calls from other sessions which are created by responders using public communications infrastructure often involving some kind of priority access as defined in Emergency Telecommunications Service (ETS) in IP Telephony [RFC4190]. By implication, this document describes the interface between the emergency services network and the Internet. This memo also describes how location may be obtained from the local access infrastructure (broadband network), and thus specifies requirements to support location in such infrastructure.

Making an emergency call involves the use of location information, referring to the physical location of the caller. Location is used within the emergency calling system to route a call to the correct PSAP, as well as by the PSAP to choose the correct responder, and direct them to the person in need of assistance.

The steps involved in an emergency call from an IP based device are (with a rough ordering of operation)

1. Device connects to access network, and obtains initial location
2. User dials visited location's emergency number
3. User device identifies call as emergency call
4. User device includes location indication (by value or by reference) in the call set-up messaging
5. emergency call set-up is routed to appropriate PSAP based on location of the caller
6. call is established with PSAP
7. caller's location is presented to PSAP operator for dispatch

As a quick overview for a typical Ethernet connected telephone using SIP signaling:

- the phone "boots" and connects to its access network
- the phone would get location from the DHCP server [an L7 server] or the first level switch's LLDP server.

- o the phone obtains the local emergency dialstring(s) from the [I-D.ietf-ecrit-lost] server.
- o It recognizes an emergency call from the dialstrings and uses "urn:service:sos" to mark an emergency call.
- o It would determine the PSAP's URI by using the [I-D.ietf-ecrit-lost] mapping server from the location provided
- o It would put its location in the SIP INVITE as a PIDF-LO in the body of the INVITE (or a reference to location in a Location header) [I-D.ietf-sip-location-conveyance] and forward the call to its first hop proxy.
- o The proxy recognizes the call as an emergency call and routes the call using normal SIP routing mechanisms.
- o The call is established and common media streams opened.

Best Current Practice for SIP user agents including handling of audio and real-time text [RFC4103]media detailed in [RFC4504] SHOULD be applied. This memo can be considered an addition to it for endpoints.

3. Which devices and services should support emergency calls

Support for voice calls and real-time text calls placed through PSTN facilities or systems connected to the PSTN is found in present PSAPs. Future PSAPs will however support Internet connectivity and a wider range of media types and provide higher functionality.. In general, if a user could reasonably expect to be able to call for help with the device, then the device or service should support emergency calling. Certainly, any device or service that looks like and works like a telephone (wired or mobile) should support emergency calling, but increasingly, users have expectations that other devices and services should work.

Using current (evolving) standards, devices that create media sessions and exchange audio, video and/or text, and have the capability to establish sessions to a wide variety of addresses, and communicate over private IP networks or the Internet, should support emergency calls.

4. Location

Location is central to the operation of emergency services. Location is used to route a call to the PSAP that serves the location, and it is used to dispatch responders to the person in need of help. It is frequently the case that the user in an emergency is unable to provide a unique, valid location themselves. For this reason, automatic location is the norm.

In Internet emergency calling, we "Determine" where the endpoint is located using a variety of measurement or wiretracing methods. We "Configure" endpoints with their own location. We "Map" the location to the URI to send the call to, and we "Convey" the location to the PSAP (and other elements) in the signaling. These topics are detailed in [I-D.ietf-ecrit-framework].

4.1. Endpoints learn their own location

With Internet based communications services, determining where the caller is located is more problematic than in PSTN and mobile systems. Existing wired phones are tethered with a wire that is connected directly to a call control device, a circuit switch. Cellular phones are tethered via a radio channel to a cell tower, which connects that cell phone to a circuit switch. The primary difficulty with IP based phones is that the connectivity, whether wired or radio channel, is decoupled from the call control device. The communications service may not have any relationship with the access network carrier, and, with NAT and VPN tunnels, may have no way to even find out who the access carrier is.

For this reason, standards have been created for endpoints (devices) to obtain location information where it is the access network that knows the location of the endpoint. To obtain location information, the endpoint can use a Location Configuration Protocol. The endpoint is a subscriber to both the access network and the communications service, and thus is in a position to obtain its location from the access network, and supply it to the communications service. These issues, and the necessity for endpoints and access networks to support LCPs is detailed in [I-D.ietf-ecrit-framework].

4.2. Location Configuration Protocols

For devices that operate on a network where the network operator controls the specification of every device connected to that network that could be used for emergency calls, the method by which location is determined need not be an IETF standard, but can be any method that achieves the desired result. Such a method MUST be specified, and every device MUST support it. It is recommended that, in addition, the network SHOULD support one or more of DHCP, [Placeholder for L7 LCP} or LLDP-MED.

For all other devices, the device MUST support DHCP, [Placeholder for L7 LCP] and LLDP-MED. The access network MUST support at least one of these.

DHCP [RFC2131] has been enhanced to provide the location of a device. [RFC3825] describes how a geo-location (lat/lon/alt) may be obtained

and [RFC4676] describes how a civic (street address) location can be obtained via DHCP.

[Placeholder for HELD, RELO or other L7 location determination methods]

[LLDP] with [LLDP-MED] extensions provides location configuration applicable in many enterprise environments.

For devices that operate in a network where the network operator controls the specification of every device connected to that network, but the network attachment supports upstream networks to which communications devices are connected (such as any network that supports Ethernet connected telephones and terminal adapters), the method by which location is determined need not be an IETF standard, but can be any method which achieves the desired result. However, the network attachment MUST support at least one of DHCP [L7 LCP] or LLDP-MED for upstream communications devices to obtain location. For smaller interior (e.g, LAN) networks, the DHCP, [L7 LCP] or LLDP-MED server should simply repeat the location obtained from the access network. For larger networks, other mechanisms, such as a DHCP Relay Agent [RFC3046] SHOULD be used to provide more accurate location of endpoints.

4.3. Self reported Location

Self reported location, where a user enters location himself, is generally unacceptable in emergency calls, although it is being used prior to automatic location determination schemes being fielded. Local laws may govern what is acceptable in any country or area. Devices and/or access networks SHOULD support a manual method to "override" the location the access network determines. The access network generally only knows the location of its demarcation point between the access network and the subscriber. The subscriber could have an extended network behind the demarc unknown to the access network. A method to account for this condition SHOULD be provided.

4.4. When Location should be Configured

Devices SHOULD get location immediately after obtaining local network configuration information. It is essential for the location to be determined BEFORE any VPN tunnels are established. It is equally essential that this location information is *not* overwritten by any process engaged from establishing a VPN connection. In other words, the established VPN to Chicago from the device in Dallas MUST NOT overwrite the Dallas location for any reason especially an emergency call.

It is desirable that location information be periodically refreshed. For devices which are not expected to roam, refreshing on the order of once per day is RECOMMENDED. For devices which roam, refresh of location SHOULD be more frequent, with the frequency related to the mobility of the device and the ability of the access network to support the refresh operation. There can be instances in which a device is aware of when it moves, for example when it changes access points. When this type of event occurs, the device SHOULD refresh its location.

It is desirable for location information to be requested immediately before placing an emergency call. However, if there is any delay in getting more recent location, the call SHOULD be placed with the most recent location information the device has. It is RECOMMENDED that the device not wait longer than 1 sec to obtain updated location, and systems should ideally be designed such that the typical response is under 100ms. These numbers are empirically derived, but are intended to keep total call signaling time below 2 seconds. There are conflicts between the time it takes to generate location when measuring techniques are used and the desire to route the call quickly. If an accurate location cannot be determined quickly, a rough location SHOULD be returned within 100ms which can be used to route the call. The location of the nearest base station in a wireless network is an example of a rough location.

4.5. Other location considerations

If the LCP does not return location in the form of a PIDF-LO [RFC4119], the endpoint MUST map the location information it receives from the configuration protocol to a PIDF-LO.

To prevent against spoofing of the DHCP server, devices implementing DHCP for location configuration SHOULD use [RFC3118].

5. Determining an emergency call

An emergency call is distinguished by the device (or a downstream element) by an "address", which in most cases for Internet connected devices is still a dialstring, although other user interfaces may be used.

Note: It is undesirable to have a single "button" emergency call user interface element. These mechanisms have a very high false call rate. PSAPs prefer devices to use their local emergency call dialstring.

While in some countries there is a single 3 digit dialstring that is

used for all emergency calls (i.e. 911 in North America), in some countries there are several 3 digit numbers used for different types of calls. For example, in Switzerland, 117 is used to call police, 118 is used to call the fire brigade, and 144 is used for emergency medical assistance. In other countries, there are no "short codes" or "service codes" for 3 digit dialing of emergency services and local (PSTN) numbers are used.

[I-D.ietf-ecrit-service-urn] introduces a universal emergency service URN scheme. On the wire, emergency calls SHOULD include this type of URI as a Route header [RFC3261]. The scheme includes a single emergency URN (urn:service:sos) and responder specific ones (urn:service:sos.police). Using the service:sos URN scheme, emergency calls can be recognized as such throughout the Internet.

Devices MUST use the service:sos URN scheme to mark emergency calls.

To determine which calls are emergency calls, some entity needs to map a user entered dialstring into this URN scheme. A user may "dial" 1-1-2, but the call would be sent to urn:service:sos. This mapping is SHOULD performed at the endpoint device, but MAY be performed at an intermediate entity (such as a SIP proxy server).

Note: It is strongly RECOMMENDED that devices recognize the emergency dialstring(s) and map to the universal emergency URN. If devices cannot do "dial plan interpretation", then the first signaling aware element (first hop proxy in SIP signaled devices) SHOULD do the mapping. It is important to not require a large number of active elements handle a call before it is recognized as an emergency call

In systems that support roaming, there may be a concept of "visited" and "home" networks. Even when there is not a "visited network", the user may be roaming (or nomadic) in a different country from their home. This gives rise to the problem of which dialstring(s) to recognize, the "home" or "visited"? While the "home" dialstrings SHOULD be recognized, it is required (by law in some countries) that the "visited" dialstrings MUST be recognized. "Visited" dialstrings would be essential if a guest used a roaming phone. Dial plan interpretation may need to take "visited" emergency dialstrings into account.

To give an example of this difference in dialstrings: If the device is from North America, the home and visited emergency dialstring is "9-1-1". If that devices roams to the UK, the home emergency dialstring is still "9-1-1", but the visited emergency dialstring would become "9-9-9". If the device roams to Paris, the home dialstring remains the same, "9-1-1", but the visited dialstring changes from 999 to "1-1-2".

The home emergency dialstrings MAY be provisioned into the device (or other element doing dialstring to universal emergency call URN mapping). [I-D.ietf-ecrit-lost]) provides dialstrings for a given location and SHOULD be used by devices to learn the local (i.e. "visited" dialstrings. "Home" dialstrings MAY be learned by configuration.

6. Session Signaling

SIP signaling [RFC3261] is expected be supported by upgraded PSAPs. Gateways MAY be used between Internet connected devices and older PSAPs. Some countries may support other signaling protocols into PSAPs.

6.1. SIP signaling requirements for User Agents

The initial SIP signaling Method is an INVITE.

1. The Request URI SHOULD be a PSAP URI obtained from LoST (see Section 6.3). If the device cannot access a LoST server, the To: SHOULD be a service URN in the "sos" tree. If the device cannot do local dialstring interpretation, the Request-URI SHOULD be a dialstring URI [I-D.rosen-iptel-dialstring]with the dialed digits. A sips URI [RFC3261] MUST be specified, unless the operation must be retried due to a failure to establish a TLS connection.
2. The To: header MUST be present and SHOULD be a service URN in the "sos" tree. If the device cannot do local dialstring interpretation, the To: SHOULD be a dialstring URI with the dialed digits. sips MUST be specified, unless the operation must be retried due to a failure to establish a TLS connection.
3. The From: header MUST be present and SHOULD be the AoR of the caller.

   NOTE: unintialized devices may not have an AoR available
4. A Via: header MUST be present and SHOULD include the URI of the device
5. A Route header SHOULD be present with the service URN in the "sos" tree, and the loose route parameter.
6. Either a P-Asserted-Identity [RFC3325] or an Identity header [RFC4474], or both, SHOULD be included to identify the sender.
7. A Contact header MUST be present (which might contain a GRUU [I-D.ietf-sip-gruu]) to permit an immediate call-back to the specific device which placed the emergency call.
8. Other headers MAY be included as per normal sip behavior
9. A Supported: header MUST be included with the 'geolocation' option tag [I-D.ietf-sip-location-conveyance], unless the device does not understand the concept of SIP Location.

10. If the device's location is by-reference, a Geolocation: header [I-D.ietf-sip-location-conveyance] MUST be present containing the URI of the PIDF-LO reference for that device. Whichever location is used for routing the message towards the PSAP or ESRP, even if there is only one, the Geolocation "message-routed-on-this-uri" header parameter SHOULD be added to the corresponding URI in the Geolocation header.
11. if a device understands the SIP Location Conveyance [I-D.ietf-sip-location-conveyance] extension and has its location available, it MUST include location either by-value or by-reference. If it is by-value, the INVITE contains a Supported header with a "geolocation" option tag, and a "cid-URL" [RFC2396] as the value in the Geolocation header, indicating which message body part contains the PIDF-LO. If the INVITE contains a location by-reference, it includes the same Supported header with the "geolocation" option tag, and includes the URI of the PIDF-LO on a remote node in a Geolocation header. [I-D.ietf-geopriv-pdif-lo-profile] MUST be used
12. If a device understands the SIP Location Conveyance extension and has its location unavailable or unknown to that device, it MUST include a Supported header with a "geolocation" option tag, and not include a Geolocation header, and not include a PIDF-LO message body.
13. A normal SDP offer SHOULD be included in the INVITE. The offer MUST include the G.711 codec, see Section 8.
14. If the device includes location-by-value, the UA MUST support multipart message bodies, since SDP will likely be also in the INVITE.
15. A UAC SHOULD include the Geolocation "inserted-by=endpoint" header parameter. This informs downstream elements which device entered the location at this URI (either cid-URL or location-by-reference URI).

6.2. SIP signaling requirements for proxy servers and B2BUAs

SIP Proxy servers processing emergency calls:

1. If the proxy does dial plan interpretation on behalf of user agents, the proxy MUST look for the local emergency dialstring at the location of the end device. If it finds it it MUST:
   * Obtain the location (or a reference to it) for the endpoint
   * Insert a Geolocation header as per 10-12 above
   * Include the Geolocation "inserted-by=server" AND "routed-by-this-uri" parameters.
   * Map the location to a PSAP uri using LoST.
   * Add a Route header with the service URN appropriate for the emergency dialstring.

   * Replace the Request-URI (which was the dialstring) with the PSAP URI obtained from LoST.
   * Route the call using normal SIP routing mechanisms.

2. The "inserted-by=" header parameter MUST NOT be modified or deleted in transit.
3. If a Geolocation "message-routed-on-this-uri" header parameter exists when a new SIP server processes a message, and the message is routing is now to be done based on another Geolocation URI (by-value or by-reference), the "message-routed-on-this-uri" header parameter MUST be removed from the old Geolocation URI and inserted with the now applicable location URI in the Geolocation header.

6.3. Mapping from Location to a PSAP URI

To route an emergency call, we make use of the [I-D.ietf-ecrit-lost] mapping service which takes a location expressed by a PIDF-LO and returns one or more PSAP URIs. The request includes the service URN which is used to determine which entity should receive the call. Ideally, mapping from location to the PSAP URI would be accomplished at the time the emergency call is placed. However, it could be that when the emergency occurs, the LoST server is unavailable to the caller, or busy. To guard against that, devices MUST cache a mapping. The mapping MUST be performed at boot time, and whenever the location changes such that the previous mapping may no longer valid. To facilitate this operation, LoST provides a mechanism that a device can use to determine when it should refresh the mapping. Devices where location changes SHOULD use this mechanism to maintain a desired mapping.

User agents that can obtain location information MUST perform the mapping from location information to PSAP URI using [I-D.ietf-ecrit-lost]. The mapping is performed whenever the UA acquires new location information that is outside the bounds of the current PSAP coverage region specified in the LoST response or the time-to-live value of that response has expired.

Determining when the device leaves the area provided by the LoST service can tax small mobile devices. For this reason, the LoST server SHOULD return a simple (small number of points) polygon for geo reported location. This can be an enclosing subset of the area when the reported point is not near an edge, or a smaller edge section when the reported location is near an edge. Civic location is uncommon for mobile devices, but reporting that the same mapping is good within a community name, or even a street, may be very helpful for WiFi connected devices that roam and obtain civic location from the AP they are connected to.

All proxies in the outbound path SHOULD recognize emergency calls with a Request URI of the service URN in the "sos" tree. A proxy recognizing such a call (which indicates that the endpoint understood the call was an emergency call, but was unable to map its location to a PSAP URI) MUST perform the LoST mapping and retarget the call to the PSAP URI (the service URN SHOULD remain as a Route header).

To deal with old user agents that predate this specification and with UAs that do not have access to their own location data, proxies that recognize a call as an emergency call that is not marked as such (see Section 5) or where the Request-URI is a service:sos URN MUST also perform this mapping, with the best location it has available for the endpoint. The resulting PSAP URI would become the Request URI.

6.4. Routing the call

Normal routing mechanisms for the specified URI should be used. For SIP signaled devices, the domain of the URI should be extracted, and the DNS consulted for a sip (or sips) SRV. The resulting NAPTR, if present, should be used for the FQDN of the server.

6.5. Responding to PSAP signaling

The PSAP is expected to use normal signaling (e.g. SIP) as per IETF standards. Devices and proxies should expect to:

1. Be REFERed to a conference bridge; PSAPs often include dispatchers, responders or specialists on a call.
2. Be REFERed to a secondary PSAP. Some responder's dispatchers are not located in the primary PSAP. The call may have to be transferred to another PSAP. Most often this will be an attended transfer, or a bridged transfer.
3. (For devices that are Mobile) SUBSCRIBE to the Presence of the AoR (or equivalent for other signaling schemes) to get location updates.
4. Support Session Timer (or equivalent) to guard against session corruption

Devices with an active emergency call (i.e. SIP Dialog) MUST NOT generate a BYE request (or equivalent for other non-SIP signaling). The PSAP must be the only entity that can terminate a call. If the user "hangs up" an emergency call, the device should ring, and when answered, reconnect the caller to the PSAP.

There can be a case where the session signaling path is lost, and the user agent does not receive the BYE. If the call is hung up, the session timer expires, and 5 minutes elapses from the last message received by the device from the PSAP, the call may be declared lost. If in the 5 minute interval an incoming call is received from the

domain of the PSAP, the device should drop the old call and alert for the (new) incoming call.

6.6. Disabling of features

The calling device and/or service SHOULD disable outgoing call features such as:

- o Call Waiting
- o Call Transfer
- o Three Way Call
- o Flash hold
- o Outbound Call Blocking

The emergency dialstrings SHOULD NOT be permitted in Call Forward numbers or speed dial lists.

The device and/or service SHOULD disable the following incoming call features on calls from the PSAP:

- o Call Waiting (all kinds)
- o Do Not Disturb
- o Call Forward (all kinds) (if the PSAP calls back within some (30min) interval)

7. Location Update

Devices which are mobile may not be able to report an accurate location when an emergency call is placed. Some deployments of location measurement are not always on, and when an emergency call is initiated, the time to get an accurate "first fix" may be several seconds. That is too long to wait to begin processing of the call. In such cases, a fast fix, or the location of a tower serving a wireless mobile device may be used to route the call, with accurate location coming later on, after the call is answered. It is possible that the PSAP that should handle the call once the accurate location is available is different from the PSAP serving the tower or the first fix location.

Mobile devices may be moving while an emergency call is in progress. The PSAPs, and/or the responders may change as the location changes.

For these reasons, and others, update of location is needed. Generally, updates should occur after the call is completed. The PSAP controls location update. For calls sent with location-by-value, the PSAP MAY reINVITE the endpoint and the 200 OK from the endpoint MUST include the location. For calls send with location-by-reference, with a SIP or SIPS scheme, the server resolving the reference MUST support a SUBSCRIBE [RFC3118] to the presence event

[RFC3856]. For other location-by-reference schemes, a repeated location dereference by the PSAP MUST be supported.

8. Media

Endpoints MUST send and receive media streams on RTP [RFC3550]. Traditionally, voice has been the only media stream accepted by PSAPs. In some countries, text, in the form of BAUDOT codes or similar tone encoded signaling within a voiceband is accepted ("TTY") for persons who have hearing disabilities. With the Internet comes a wider array of potential media which a PSAP should accept. Using SIP signaling includes the capability to negotiate media. Normal SIP offer/answer [RFC3264] negotiations MUST be used to agree on the media streams to be used.

Endpoints supporting voice MUST support G.711 A law (and mu Law in North America) encoded voice as described in [RFC3551]. It is desirable to support wideband codecs in the offer Silence suppression (Voice Activity Detection methods) MUST NOT be used on emergency calls. PSAP call takers sometimes get information on what is happening in the background to determine how to process the call.

Newer text forms are rapidly appearing, with Instant Messaging now very common, endpoints supporting IM MUST support either [RFC3428] or [RFC3920]. Endpoints supporting real-time text MUST use [RFC4103]. The expectations for emergency service support for the real-time text medium, described in [I-D.ietf-sipping-toip], section 7.1 SHOULD be fulfilled.

Video may be important to support Video Relay Service (Sign language interpretation) as well as modern video phones. Endpoints supporting video MUST support H.264 per [RFC3984].

9. Testing

9.1. Testing Mechanism

INVITE requests to a service urn with a urn parameter of "test" indicates a request for an automated test. For example, "urn:service.sos.fire;test". As in standard SIP, a 200 (OK) response indicates that the address was recognized and a 404 (Not found) that it was not. A 486 (Busy Here) MUST be returned if the test service is busy, and a 488 (Not Acceptable Here) MUST be returned if the PSAP does not support the test mechanism.

In its response to the test, the PSAP MAY include a text body

indicating the identity of the PSAP, the requested service, and the location reported with the call. For the latter, the PSAP SHOULD return location-by-value even if the original location delivered with the test was by-reference.

A PSAP accepting a test call SHOULD accept a media loopback test[I-D.ietf-mmusic-media-loopback] and SHOULD support the "rtp-pkt-loopback" and "rtp-start-loopback" options. The user agent would specify a loopback attribute of "loopback-source", the PSAP being the mirror. User Agents should expect the PSAP to loop back no more than 3 packets of each media type accepted, after which the PSAP would normally send BYE.

User agents SHOULD perform a full call test, including media loopback, after a disconnect and subsequent change in IP address. After an initial IP address assignment test, a full test SHOULD be repeated approximately every 30 days with a random interval.

User agents MUST NOT place a test call immediately after booting, as a widespread power outage and subsequent restoration would impose an inordinate load on the emergency call routing system.

PSAPs MAY refuse repeated requests for test from the same device in a short period of time.

10. Security Considerations

There are no new security considerations beyond those in the normative references. This memo does not introduce any new protocols; it specifies use of several of them.

10.1. Threats against endpoints

The largest threat against the endpoint is inadvertent disclosure of its location. The endpoint acquires location from a Location Configuration Protocol. Some of the protocols are very limited as to the scope which messages within the protocol are distributed. DHCP for example is limited to the local subnet. LLDP is limited to the link. The [L7 LCP] is not limited and TLS SHOULD be used to protect location privacy.

The location configuration server could be spoofed, thus providing wrong location, and misdirecting help when an emergency call is placed. When DHCP is the LCP [RFC3118] SHOULD be used to prevent spoofing if possible. LLDP server spoofing would be limited to devices connected to the link and is not seen as a credible threat. Deployments should limit hubs and downstream switches to IP connected

devices that could be used to place emergency calls. [L7 LCP] SHOULD use DIGEST authentication (or better) to identify the LIS.

The LoST server, which is the source of Location to PSAP URI mapping, and local dialstrings, could be spoofed. Use of DHCP to obtain the location of the server limits the ability to misdirect the user. LoST protocol use SHOULD include TLS with server certs to prevent spoofing.

The PSAP could be spoofed. Client SHOULD use TLS with server certs to prevent spoofing.

10.2. Threats against the Emergency Service

The largest threats to the Emergency Service are forgery of location and denial of service attacks on the PSAP and/or ESRP.

To mitigate forgery of location, location object SHOULD be signed. Since access networks and PSAPs are usually local to each other, providing a PKI should not be onerous for many residential deployments. However, enterprises may deploy access networks with location, which is to be encouraged. PKI covering all enterprises within a PSAP service area may be much more problematic.

To mitigate denial of service attacks, endpoint SHOULD use TLS (which implies TCP) in the signaling towards the LoST server and the PSAP/ESRP. Return routability of signaling would help significantly. Use of P-Asserted-Identity or SIP Identity is also REQUIRED of calling networks.

11. Normative References

[I-D.ietf-ecrit-framework]
Rosen, B., "Framework for Emergency Calling in Internet Multimedia", draft-ietf-ecrit-framework-00 (work in progress), October 2006.

[I-D.ietf-ecrit-lost]
Hardie, T., "LoST: A Location-to-Service Translation Protocol", draft-ietf-ecrit-lost-04 (work in progress), February 2007.

[I-D.ietf-ecrit-service-urn]
Schulzrinne, H., "A Uniform Resource Name (URN) for Services", draft-ietf-ecrit-service-urn-05 (work in progress), August 2006.

[I-D.ietf-geopriv-pdif-lo-profile]
Tschofenig, H., "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", draft-ietf-geopriv-pdif-lo-profile-05 (work in progress), October 2006.

[I-D.ietf-mmusic-media-loopback]
Hedayat, K., "An Extension to the Session Description Protocol (SDP) for Media Loopback", draft-ietf-mmusic-media-loopback-05 (work in progress), September 2006.

[I-D.ietf-sip-gruu]
Rosenberg, J., "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", draft-ietf-sip-gruu-11 (work in progress), October 2006.

[I-D.ietf-sip-location-conveyance]
Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", draft-ietf-sip-location-conveyance-07 (work in progress), February 2007.

[I-D.ietf-sipping-service-examples]
Johnston, A., "Session Initiation Protocol Service Examples", draft-ietf-sipping-service-examples-12 (work in progress), January 2007.

[I-D.ietf-sipping-toip]
Wijk, A. and G. Gybels, "Framework for real-time text over IP using the Session Initiation Protocol (SIP)", draft-ietf-sipping-toip-07 (work in progress), August 2006.

[I-D.rosen-iptel-dialstring]
Rosen, B., "Dialstring parameter for the Session Initiation Protocol Uniform Resource Identifier", draft-rosen-iptel-dialstring-05 (work in progress), March 2007.

[LLDP]   IEEE, "IEEE 802.1AB-2005, Station and Media Access Control Connectivity Discovery (aka Link Layer Discovery Protocol - LLDP)", May 2004.

[LLDP-MED]
TIA, "ANSI/TIA-1057, Link Layer Discovery Protocol for Media Endpoint Devices (aka LLDP-MED)", Apr 2006.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[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.

[RFC3264] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, 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.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, July 2003.

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

[RFC3856] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004.

[RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, October 2004.

[RFC3984] Wenger, S., Hannuksela, M., Stockhammer, T., Westerlund, M., and D. Singer, "RTP Payload Format for H.264 Video", RFC 3984, February 2005.

[RFC4103] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", RFC 4103, June 2005.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[RFC4190] Carlberg, K., Brown, I., and C. Beard, "Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony", RFC 4190, November 2005.

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

[RFC4504] Sinnreich, H., Lass, S., and C. Stredicke, "SIP Telephony Device Requirements and Configuration", RFC 4504, May 2006.

[RFC4676] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4676, October 2006.

Authors' Addresses

Brian Rosen
NeuStar
470 Conrad Dr.
Mars, PA 16046
US

Phone: +1 724 382 1051
Email: br@brianrosen.net

James M. Polk
Cisco Systems
3913 Treemont Circle
Colleyville, TX 76034
US

Phone: +1-817-271-3552
Email: jmpolk@cisco.com

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).