

ECRIT
Internet-Draft
Expires: January 19, 2006

H. Tschofenig
Siemens
H. Schulzrinne
Columbia U.
M. Shanmugam
TUHH
July 18, 2005

Security Threats and Requirements for Emergency Calling
draft-tschofenig-ecrit-security-threats-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 19, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

With the increasing interest to replace parts of the public switched telephone network (PSTN) with the IP-based network, the core functionality of PSTN such as emergency services, has to be offered when using IP-based technologies. Since the PSTN and the Internet follow different design principles their architecture is quite

Internet-Draft

Threats and Req. for Emergency

July 2005

different. This fact has to be considered and security threats for an IP-based emergency environment have to be re-evaluated. This document investigates the potential threats against the IP based emergency architecture. It focuses on some analysis of threats for both the end hosts and the infrastructure that aims to support emergency services.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Motivations of Attackers of ECRIT	5
4.	Basic Actors	6
5.	Security Threats	9
5.1	Denial of Service Attacks	9
5.2	Call Identity Spoofing	9
5.3	Location Spoofing	10
5.4	Impersonating a PSAP	10
5.5	Signaling Message Modification	11
5.6	Modification of the Emergency Call	11
5.7	Loss of confidentiality	11
5.8	Replay Attack	11
5.9	Corrupting Configuration Information	12
5.10	Corrupting Database Information	12
6.	Security Requirements	13
6.1	Denial of Service Attacks	13
6.2	Call Identity Spoofing	14
6.3	Location Spoofing	14
6.4	Impersonating a PSAP	16
6.5	Signaling Message Modification	16
6.6	Replay Attack	17
6.7	Loss of confidentiality	17
6.8	Modification of the Emergency Call	17
6.9	Corrupting Configuration Information	17
6.10	Corrupting Database Information	18
6.11	Location Validation and Verification	18
7.	Security Considerations	20
8.	IANA Considerations	21
9.	References	22
9.1	Normative References	22
9.2	Informative References	22
	Authors' Addresses	22
	Intellectual Property and Copyright Statements	23

1. Introduction

This document provides an overview of security mechanisms and motivations for using them in the VoIP-based emergency services. PSTN users can summon help for emergency services such as ambulance, fire and police using a well known unique number (e.g., 911 in North America, 112 in in Europe). With the introduction of IP-based telephony support for emergency service also has to be provided. A number of protocols and protocol extensions need to interwork in order to provide emergency functionality.

Since the Internet is hostile place, it is important to understand the security threats for emergency services. Otherwise, an adversary can use the infrastructure to place fraudulent calls, mount denial of service attacks, etc.

This document focuses on the security threats and security requirements for the IP-based emergency service infrastructure only without interaction with PSTN infrastructure elements.

A few discussions within this document are related to emergency handling but solutions will not be developed as part of the ECRIT working group. Hence, the are included mainly for completeness and to point to the need to investigate additional aspects. Depending on the chosen protocols (for the emergency call itself, for directory access related to emergency call routing, for obtaining location information from the network, etc.) various solutions might also already be available to fulfill these security requirements and to address the threats appropriately.

This document is organized as follows: [Section 2](#) describes basic terminology, [Section 5](#) illustrates security threats and [Section 6](#) lists security requirements.

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 Caller, Public Safety Answering Point (PSAP), Access Infrastructure Provider, Application (Voice) Service Provider, Emergency Call Taker, etc. is taken from [[I-D.schulzrinne-ecrit-requirements](#)].

Additionally, we use the following terms throughout the document:

Emergency Call Routing Support: This term refers to entities that route the emergency call to the appropriate PSAP based on information like location information, language, etc. If SIP is used as a protocol for session setup and call routing, for example, then this entity would correspond to a SIP proxy.

Directory: This entity refers to a distributed directory protocol. DNS is one example of such as distributed directory but there are other protocols that might fulfill the requirements listed in [[I-D.schulzrinne-ecrit-requirements](#)] for such a protocol.

Asserted Location Information: The term asserted location information refers to the property that the recipient of such an object is able to verify that it was generated by a particular party that is authorized to do so.

3. Motivations of Attackers of ECRIT

The most obvious motivation for an attacker, in the context of emergency, is to hinder user(s) not to avail the emergency service. This can be done by variety of means such as impersonating a PSAP, directory server, forging or spoofing location, identity etc., However, there are several other potential motivations that cause concern. Attackers might also wish to learn the nature emergency information by eavesdropping an emergency call in order to reuse or extract the relevant information that might cause potential problems to the end hosts such as replay attacks, revealing the identity of the user.

Attackers may want to prevent or delay an emergency caller by modifying some information in the message typically modifying the location of the caller, while placing the emergency call. In some cases, this will lead the emergency responders to dispatch the services to the spoofed area and might not be available to the other callers. It might also be possible for an attacker to impede the users not to reach an appropriate PSAP by corrupting or modifying the location of an end host or the information returned from the mapping protocol. Since the regulatory aspects of the emergency call often

does not mandate authentication of the caller, it is easy for an attacker to forge some data(location information) to an PSAP, thereby forcing the emergency responders to dispatch the services, which might cause a denial of service to its legitimate users.

Finally, some attackers may simply want to halt the operation of an entire emergency architecture through denial-of-service attacks.

[4.](#) Basic Actors

In order to support emergency services covering a large physical area various infrastructure elements are necessary: Access Infrastructure Providers, Application (Voice) Service Provider, PSAPs as endpoints for emergency calls, directory services or other infrastructure elements that assist in during the call routing and potentially many other entities.

This section outlines which entities will be considered in the threat analysis and shows the high level architecture.

Location
Information +-----+

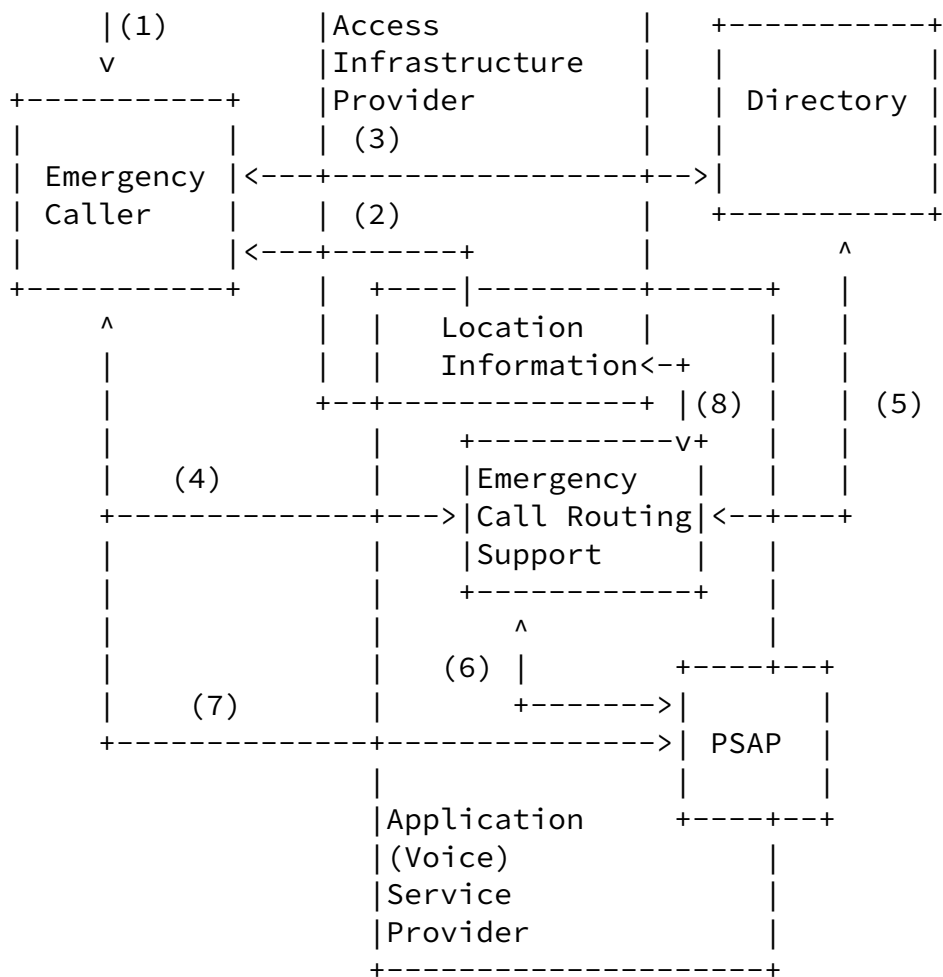


Figure 1: Framework

Figure 1 shows the interaction between the entities involved in the call. There are a number of different deployment choices, as it can be easily seen from the figure. The following deployment choices need to be highlighted:

- o How is location information provided to the end host? It might either be known to the end host itself (due to manual configuration or provided via GPS) or available via a third party. Even if location information is known to the network it might be made available to the end host. Alternatively, location information is used as part of call routing and inserted by intermediaries.

- o Is the Access Infrastructure Provider also the Application (Voice) Service Provider? In the Internet today these roles are typically provided by different entities. As a consequence, the Application (Voice) Service Provider is typically not able to learn the physical location of the Emergency Caller.

Please note that the overlapping squares aim to indicate that certain functionality can be collapsed into a single entity. As an example, the Application (Voice) Service Provider might be the same entity as the Access Infrastructure Provider and they might also operate the PSAP. There is, however, no requirement that this must be the case. Additionally it is worth pointing out that end systems might be its own VoSP, e.g., for enterprises or residential users.

Below, we describe various interactions between the entities shown in Figure 1 are described:

- o (1) Location information might be available to the end host itself.
- o (2) Location information might, however, also be obtained from the Access Infrastructure Provider (e.g., using DHCP or application layer signaling protocols).
- o (3) The Emergency Caller might need to consult a directory to determine the PSAP that is appropriate for the physical location of the emergency caller (and considering other attributes such as a certain language support by the Emergency Call Takers).
- o (4) The Emergency Caller might get assistance for emergency call routing by infrastructure elements (referred as Emergency Call Routing Support entities). In case of SIP these entities are proxies.
- o (5) Individual Emergency Call Routing Support entities might need to consult a directory to determine where to route the emergency call.
- o (6) The Emergency Call Routing Support entities need to finally forward the call, if infrastructure based emergency call routing

- o (7) The emergency caller might interact directly with the PSAP without any Emergency Call Routing Support entities.

[5.](#) Security Threats

This section discusses various security threats related to emergency call handling.

[5.1](#) Denial of Service Attacks

A (distributed) denial-of-service attack (DoS attack) on a PSAP, for example, might isolate the PSAP from the Internet, for a while, thus unable to receive the emergency calls at that time. Since a particular PSAP is responsible for a certain geographical boundary, attacking a single PSAP means denying the service to the entire area (if no other backup PSAP is available). DoS attacks might appear in many different flavors ranging from standard SYN floodings to attacks where a human operator is involved then he has to determine whether a call is in fact a true emergency call. In some cases this might lead the case where the emergency staff (police, ambulance, etc.,) might need to rush to the indicated emergency scene (potentially an arbitrary location) and will therefore not be available for other rescue assignments during that time.

As such, PSAPs can be seen as a particularly valuable target since the consequences of an unreachable PSAP has severe consequences.

Attacks against the routing infrastructure enables an adversary to prevent all nodes attached to this network to sent emergency calls. Attacks against entities that assist in the call routing (such as attacks against the directory service) might make it difficult or impossible for emergency call to reach its intended PSAP.

[5.2](#) Call Identity Spoofing

If an adversary is able to make emergency calls without the need to disclose its identity (such as a SIP URI or NAI) then prank calls cannot be traced back. If the call is proxy-routed, the PSAP will not see the IP address of the caller in signaling. Additionally, it might be necessary for the Emergency Call Taker to initiate a voice, video or instant messaging exchange towards the Emergency Caller.

Trying to find an adversary that placed a crank call is difficult if somebody uses an open 802.11 access point, even if you can find the owner of that access point. This problem is no different than somebody placing an emergency call from a payphone.

If the adversary is never authenticated (neither to the PSAP nor to the Access Infrastructure Provider) then it is possible to trace the

call back to a make a particular entity accountable.

A standard requirement for emergency systems is that emergency calls must also be placed in absence of any authentication. An adversary will typically exploit these weaknesses and he will always find networks that do not perform network access authentication of the user prior to providing network access. As such, the emergency infrastructure cannot neither rely on network access authentication nor on authentication of the caller towards the PSAP or the Application (Voice) Service Provider.

It is necessary to point to the fact that authentication in the emergency case might require the authorization procedure to be skipped. For example, in an emergency case it is still possible to authenticate the user of an emergency call but without considering that its credits are exhausted.

[5.3](#) Location Spoofing

An adversary might want to made-up faked location information in order to fool the emergency personnel. This is made particularly easy if the location information is provided by the Emergency Caller either via manual configuration or via GPS. Spoofing is more difficult if an entity providing Emergency Call Routing Support inserts location information into emergency call signaling. In this case the adversary needs to route the call via some intermediaries. This is possible since these devices are often, by their nature as IP devices, addressable from an arbitrary physical location. The usage of VPN (or other tunneling mechanisms) and proxies further complicates the ability to infer the physical location from the IP address seen by the PSAP.

[5.4](#) Impersonating a PSAP

An adversary might pretend to operate a PSAP. When either an end host or an intermediate device wants to determine the PSAP that is responsible for a particular geographical area by sending a query to the directory an adversary might return a faked response. Returning an incorrect response message does not require the adversary to be somewhere along the path. It is sufficient for an adversary to be located in a broadcast medium and the adversary has to reply as soon

as a query is observed (if no security protection is utilized). If the response indicates a legitimate but inappropriate (i.e., a PSAP that is authoritative for a different geographical area) then the emergency call interaction will be able to continue but will suffer from delays until the emergency call can be forwarded to the correct PSAP, potentially involving human interaction (by the Emergency Call Taker).

[5.5](#) Signaling Message Modification

An adversary that is located along the signaling path might modify the content of emergency calls, such as location information or identity information. This might lead to a denial of service attack against the emergency personell, disruption of the emergency call, delayed call setup, etc.

An adversary might want to inject signaling messages to terminate or redirect the call to another location. Dropping or delaying signaling messages is also possible for an on-path adversary.

Depending on the capability of the signaling protocol the range of possible attacks might have been documented already.

[5.6](#) Modification of the Emergency Call

An adversary along the media path might want to modify the data traffic part of the emergency call (voice, video or instant message). An attacker can change the message on-the-fly and fool the PSAP to receive meaningless or bogus messages. The response messages to Emergency Caller might also be subject to change, for example by injecting a recorded failure message.

[5.7](#) Loss of confidentiality

An adversary might eavesdrop an emergency call and use the information to future sessions as part of replay attacks. The ability to eavesdrop also allows to learn details about the emergency situation which might be of interest for the press or other media organizations. Please note that the location of the adversary is important regarding the eavesdropped area. For example, an adversary

in a WLAN is typically able to see a small amount of traffic due to the coverage area of typical WLAN network.

Reavealing the true identity of the user as part of the privacy override mechanism might conflict with the users privacy settings.

[5.8](#) Replay Attack

An adversary might want to use eavesdropped information to mount attacks in the future. This might be necessary if information cannot be re-created by the adversary (for example, asserted location information). The ability to replay messages or individual objects the specific property of these messages and objects is important. For example, asserted location information might bind location information and a timestamp with a digital signature together that makes it difficult to reuse this object beyonds its lifetime.

Tschofenig, et al.

Expires January 19, 2006

[Page 11]

Internet-Draft

Threats and Req. for Emergency

July 2005

[Editor's Note: It is sometimes hard to tell what are real threats and what security threats are addressed already by certain solutions outside the scope of the working group. Addressing all standard security threats is a long process if certain mechanisms are required in an case that largely or completely mitigate against these threats.]

[5.9](#) Corrupting Configuration Information

An adversary might override all locally configured emergency numbers. This might be particular problematic if these emergency numbers are dynamically retrieved using some mechanisms. As such, an Emergency Caller would start a call that either leads to a blackhole (as such it is a DoS attack), the Emergency Caller connects to a rogue PSAP or to an inappropriate PSAP.

[5.10](#) Corrupting Database Information

An attacker might want to provide emergency callers with wrong information about emergency service contact URIs. An adversary can accomplish this goal in various ways, including message modification, spoofing or corrupting the database. Since the database provides a pointer(e.g., SIP URI) to an appropriate PSAP, care must be taken when retrieving emergency URI. A succesfull forging will lead the user to reach either a false PSAP or to a black hole.

6. Security Requirements

[Editor's Note: A few requirements below are already addressed by a number of requirements and solution specific documents today. In order to keep the document short it would be reasonable to focus only on the difficult security threats and requirements for emergency calls rather than enumerating everything that could happen to an emergency call. The working group should decide how to proceed with this particular issue and what threats and requirements should be elaborated in more detail.]

Compiling security requirements to address the threats listed in the previous section might be impacted by several constraints:

- Security mechanisms may lead to a certain performance overhead (e.g., several roundtrips).

- A certain security infrastructure is required that might lead to

deployment problems. For example, end user certificates, certificates for networks, usage of authorization certificate, etc. might need to be deployed before any of these mechanisms are useful.

Many of these aspects are related to regulatory and legal requirements that may vary from country to country. Typically, these mechanisms cannot be mandated by an IETF specification.

Some of the requirements impose solutions that are out-of-scope of the ECRIT working group.

Given the above-listed constraints the requirements that have to be addressed by work that is done within ECRIT have to be highlighted. Other requirements have to be read as 'if you would like to address this threat, then you might want to consider this requirement' rather than 'any solution must address fulfill this requirement'.

[6.1](#) Denial of Service Attacks

It is difficult to address all possible denial of service attacks that might lead to disruption of an emergency call since a number of IETF protocols are used in order to provide this functionality. Hence, care must be taken when protocol extensions are developed that the chance for a denial of service attack is not increased. Even without using any security mechanisms (such as authentication and key exchange protocols) some degree of security has to be provided.

It is important to understand that the ability to mount DoS attacks must also be considered as part of the architecture work when legal

and regulatory requirements are known and need to be fulfilled.

[6.2](#) Call Identity Spoofing

A standard requirement to prevent identity spoofing is to authenticate the Emergency Caller. Authentication mechanisms that require multiple roundtrips and as such might delay the call are often not desirable or cannot be mandated.

[6.3](#) Location Spoofing

An Emergency Caller might in many cases know its own location information because it was obtained via civic or geospatial location extensions for DHCP, via manual configuration or via GPS. Unfortunately, information provided by the end host is untrustworthy particularly when it is as important as location information. Two approaches have been discussed in the past that place lead to a few requirements:

- o Location Information is asserted by the Access Infrastructure Provider. As such, the end host might use GPS but uses a protocol to allow the network to assert the location information. This approach also has its limitations if the coverage area of the wireless network is fairly large.
- o Location Information is added to the emergency call via an Emergency Call Routing Support entity. Depending on the protocol used for call routing and on the properties of this protocol it might be necessary to return the asserted location information to the end host since intermediate nodes might not be allowed to insert objects into the call setup messages (at least not in all parts of the messages, such as bodies). These signaling entities, in general, do not know the physical location of the user. Thus, they have to rely on somebody else to actually provide the location, e.g., the Access Infrastructure Provider.

As it can be seen from these two options the main difference is based on the type of protocol that is used in the message communication. This has an impact on the semantic and on the availability of certain attributes (such as identities that are used by these protocols) and on deployment constraints. Based on the observation that the Access Infrastructure Provider is closest to the end host and is therefore the most likely entity that knows something about the physical location of the end host it seems to be reasonable to assume that some entity that asserts the location information is actually available in this particular network.

In the context of emergency, spoofing can be loosely divided into

- o wide-area spoofing - users pretend to be in Germany but actually in US.
- o local-area spoofing - users spoof location information to an

extend (few miles).

- o local-area cloning - users pretend to be in place X if they were actually there, a while ago.

The following requirements need to be provided in order for asserted location information to accomplish its goals:

- o Location Information MUST be integrity protected to prevent modifications by third parties.
- o The recipient of the asserted location information object MUST be able to determine the party that asserted the location information in order to verify the assertion. As such, authentication of the asserting party (the entity that created the assertion) MUST be provided.
- o The asserted location information MUST include a timestamp to limit its validity in order to reduce replay attacks.
- o The recipient of the asserted location information MUST have a way to verify that the asserting party is indeed authorized to create such an assertion. As such, authentication is insufficient if not further authorization decision can be associated to the authenticated identity.
- o The recipient of the asserted location information SHOULD have a mechanism to determine the Emergency Caller based on the provided assertion.

The last bullet deserves further discussion: If some information about the Emergency Caller identity has to be included, which is only for the purpose of traceability then this functionality might not be of general use. This is because an adversary will always find networks that do not authenticate the user prior to providing network access. Furthermore, the goal of a number of network access authentication protocols is to prevent disclosure of the user identity to entities other than to the user's home network. Note that the term 'user identity' does not require that this identity directly points to the 'real' identity of a user. A court might want to require this identity to be resolved and to determine the user behind this identity. Even if the access network would like to ascertain the user's identity as part of the asserted location information it is, in many cases, not even possible for the Access

Infrastructure Provider.

If the authenticated user identity is not available to the Access Infrastructure Provider then only a few other identities might be useful, such as the IP address or the MAC address. Other identities, such as the Host Identity, might not be available since they are only used by very few protocols. An assertion that indicates the network in combination with the IP and/or MAC address (together with a timestamp) might provide some limited degree of traceability only if the user was authenticated directly to this particular network. Providing the IP address allows some obvious attempts to cheat to be caught. Hence, there is the question whether some identity should be added at all given the potential limitations and the potential small amounts of cut-and-paste attacks. Using end user based authentication in addition to the asserted location information would be helpful (e.g., using end user certificates) but will impose a serious deployment problem. Given the fact that emergency calls must still be allowed even without end user authentication certainly defeats the purpose of these mechanisms. A partial attempt to address some prank calls is to classify emergency calls based on the availability of the provided attributes. If suspicious information is being provided that may well be wrong then additional verification steps need to be taken. For example, if a report of a large fire on a Manhattan street is received then the PSAP may wait to dispatch until it gets a second person to call in. This approach obviously has some limitations as well.

[6.4](#) Impersonating a PSAP

The Emergency Caller SHOULD be able to determine conclusively that he has reached an accredited emergency call center. This requirement is meant to address the threat that a rogue, possibly criminal, entity pretends to accept emergency calls and disrupts the emergency infrastructure.

- o A user agent must be able to authenticate a PSAP.

Unlike in the PSTN case IP based networks provide a better opportunity to spoof a PSAP since physical access to the cable plant is required in the PSTN case, while this may not be true for the IP case.

[6.5](#) Signaling Message Modification

To protect signaling messages against modifications either individual attributes SHOULD be protected (such as location objects) or the entire signaling message communication SHOULD experience end-to-end

protection. This requires integrity and replay protection to be

applied. Authentication of the data sender and the data receiver SHOULD be provided to prevent a man-in-the-middle attack.

[6.6](#) Replay Attack

In order to protect signaling messages (or individual attributes) to be replayed in future protocol sessions integrity and replay protection mechanisms SHOULD be provided.

[6.7](#) Loss of confidentiality

In order to prevent leakage of information exchanged during the emergency call (both signaling and data traffic) confidentiality protection SHOULD be provided. The mechanisms to accomplish this functionality are typically different for the data traffic and for the signaling messages and various scenarios, such as hop-by-hop, end-to-middle, middle-to-middle and end-to-end security, need to be considered. Particularly the key management aspects for end-to-end security mechanisms imposes a deployment burden and hence need to be critically analysed in order to determine its applicability in the given context.

[6.8](#) Modification of the Emergency Call

To protect a man-in-the-middle attack i.e disallow the adversary to modify or to inject data traffic into the communication between the Emergency Caller and the PSAP, the mechanisms like integrity, replay and data origin authentication SHOULD be provided. Since the signaling messages are used to authenticate the end points and to distribute the required keying material it is necessary that either the key exchange protocol itself and the signaling messages experience appropriate security protection. The term 'appropriate' refers to the given context, the used signaling protocol and the key exchange protocol.

Please note that the interactive nature of a voice communication already provides a some degree of protection. However, with the introduction of instant messaging the freshness of the Emergency Call needs to be provided by other means.

[6.9](#) Corrupting Configuration Information

Devices SHOULD be assured of the correctness of the local emergency numbers that are automatically configured. If we assume a fixed, global emergency service identifier that requires no configuration and only configure local "traditional" emergency numbers, users are not likely to suddenly dial some random number if a rogue configuration server introduces this as an additional emergency

Tschofenig, et al.

Expires January 19, 2006

[Page 17]

Internet-Draft

Threats and Req. for Emergency

July 2005

number. The ability to override all locally configured emergency number is of more concern. If the Emergency Caller does not use the infrastructure to route the call to the appropriate PSAP then the security of the directory service is of importance for security.

[6.10](#) Corrupting Database Information

If the mapping client i.e., the entity that requests location information using a mapping protocol accepts the emergency contact information from an unauthenticated mapping server i.e., the entity that provides location information, it is highly possible to receive bogus or prank emergency contact URIs. Particularly the caching properties of a distributed directory might be exploited. To ensure the secure retrieval of information, the following properties are assumed:

- o The mapping client MUST be able to authenticate the mapping server.
- o The interaction between the mapping client and the mapping server MUST be integrity and replay protected.
- o The mapping server MUST provide data origin authentication thereby ensuring that the provided data items are indeed from the claimed source.
- o The mapping server MUST provide information to ensure that it is authoritative for the provided information.

[6.11](#) Location Validation and Verification

location validation ensures that an address exists and is mappable to a PSAP. A valid address, however, does not imply that the call

actually originated from that location. We refer to location verification as the assurance that the call was placed at the location claimed, including any error margins provided.

Verifying a location is generally more difficult than location validation as there is currently no generally trusted service that can vouch for the location of the caller. In some cases, AIPs or ISPs may be able to indicate the location of the caller with high confidence and they may possess cryptographic certificates that are trusted by the PSAP. This may not require a global certification authority (CA), as a regional PSAP typically only deals with a modest number of larger enterprises and thus could obtain their public keys even if self-signed.

However, even if the AIP or ISP provides a signed location, it is

difficult to ensure that such a signed location object is only used for calls from that location, as it will have to be copied from a location delivery protocol to the call signaling protocol. For example, a third party could obtain such a signed location object and use it elsewhere. Naturally, timestamps will restrict such usage to the order of minutes or hours, depending on how often location information is updated. A PSAP may want to be able to answer the following questions:

- o Who originally provided this particular location information?
- o Did the call originate from that particular geospatial or civic address and who says so and how do they know?

[7.](#) Security Considerations

This document addresses security threats and security requirements. Therefore, security is considered throughout this document.

[8.](#) IANA Considerations

This document does not require actions by the IANA.

[9.](#) References

[9.1](#) Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", March 1997.

9.2 Informative References

[I-D.schulzrinne-ecrit-requirements]

Schulzrinne, H. and R. Marshall, "Requirements for
Emergency Context Resolution with Internet Technologies",
May 2005.

Authors' Addresses

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
USA

Phone: +1 212 939 7042
Email: schulzrinne@cs.columbia.edu
URI: <http://www.cs.columbia.edu/~hgs>

Murugaraj Shanmugam
Technische Universitat Hamburg-Harburg
Department of Security in Distributed applications
Harburger Schlossstrasse 20
Hamburg-Harburg 21079
Germany

Email: murugaraj.shanmugam@tuhh.de

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

