

Security in the Emergency Services Support for the IP Multimedia Subsystem (IMS)

Yacine Rebahi, Andreea Ancuta Onofrei and Thomas Magedanz,
FOKUS Fraunhofer Institut,
10589 Berlin, Germany
{yacine.rebahi, andreea.ancuta.onofrei, thomas.magedanz}@fokus.fraunhofer.de

Abstract. In this paper, we describe some concrete attacks patterns related to the IMS emergency support framework. We provide some solutions about how to deal with threats that might be carried out against emergency services in general VoIP network. The details about our implementation and how to use it are presented, as well.

Keywords: IMS, emergency services, security, DoS attacks.

1 Introduction

Evidently, telecommunications play a major role in speeding response and minimizing loss of life and property. Communications systems can help, for instance, in daily emergency calling where calls will be made to police, ambulance and fire brigade.

Next Generation Networks (NGNs), in particular the IP Multimedia Subsystem (IMS), are certainly the future replacement of the current telecommunication networks, therefore it is normal that the current emergency systems need to be upgraded in order to fulfill the NGNs requirements.

There are different standardization bodies that have been working on the evolving of the current emergency systems, namely, IETF[1], 3GPP[2], and ETSI TISPAN[3]. 3GPP is dealing with the emergency support for the IP Multimedia Subsystem (IMS) and tries to reuse at maximum the work being done within some IETF groups. In addition to that, a close collaboration is maintained between 3GPP and ETSI TISPAN in order to port the undertaken activities to fixed networks as well.

As providing assistance for persons in danger is a vital service and the information communicated between the caller and the call takers is sensitive, security seems to be mandatory when developing such services. In fact, only little and general work was achieved in this direction and it is mainly a description of the corresponding threats and some requirements for emergency call prioritization and mapping [4].

This document is divided as follows: Sections 2 and 3 provide, respectively, an overview of the IP Multimedia Subsystem and the corresponding emergency support. Section 4 discusses the security issues related to the emergency services, in particular the concrete attacks scenarios that might occur in the IMS environment. Sections 5

and 6 introduce the project in which these security issues are being implemented. Finally section 7 concludes the paper.

2 IMS Overview

The IP Multimedia Subsystem (IMS) is the key enabler in the mobile world for providing rich multimedia services to the end-users.

IMS first appeared in release 5 of the evolution from 2G to 3G networks “from W-CDMA to UMTS”. This release supports both GSM and GPRS networks. In 3GPP release 6, interworking with WLAN was added. 3GPP release 7 adds support for fixed networks, together with TISPAAN, this collaboration allowed the adoption of a more generalized model able to address a wider variety of network and service requirements. This overall architecture is based upon the concept of cooperating subsystems sharing common components [5]. This subsystem-oriented architecture enables the addition of new subsystems over the time to cover new demands and service classes

The IMS underlying network architecture can be divided into three main layers: Access Layer, Control Layer and Service Layer (see Fig. 1).

The access layer consists of IP routers and legacy PSTN switches that provide access to the IMS network both from contemporary IP telephony devices and older circuit switch devices respectively. IP devices compatible with IMS incorporate a SIP user agent that is used to place voice or video calls toward the network.

The control layer of the IMS network consists of nodes for managing call establishment, management, and release, the Call Session Control Function (CSCF) , performed by: Proxy (P-CSCF), Interrogating (I-CSCF) and Serving (S-CSCF).

Before the user can use the services from the IMS network it must authenticate itself, by performing a registration. The subscriber data of every user is located in the Home Subscriber Service (HSS), which acts as a Authentication, Authorization and Accounting (AAA) server, providing a central repository of user-related information.

The P-CSCF is the link of the User Element (UE) to the IMS network, receiving all the signaling traffic from/for the user, allowing access only to registered users.

The S-CSCF performs routing traffic towards other networks, manages billing and session expiration intervals, and interrogates the HSS to retrieve authorization, service triggering information and user profile.

The I-CSCF is in charge of querying the HSS if a specific user is present at the HSS and which S-CSCF the HSS has allocated for it.

IMS applications are hosted in the service layer. This layer consists of SIP Application Servers (AS) which provides the end user service logic. The (AS) execute IMS applications and services by manipulating SIP signaling and interfacing with other systems. Usually, the AS will offer a programming language and framework for creating new services, for example Java SIP and HTTP Servlets (more details at [2]).

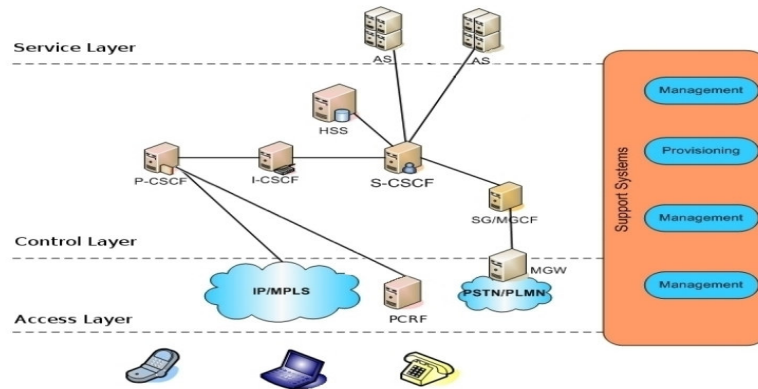


Fig. 1: IMS architecture

3 Emergency Services Support for IMS

We have chosen the IMS architecture because it answers to some important requirements:

- It supports multiple access technologies both Circuit Switched (CS) and Packet Switched (PS), which enables using the same (location, service) to (call center) mapping procedure.
- Routing the emergency call is done in the network attached to and is location aware, so the call will be routed to the nearest call center and the PSAP can right from the start of the conversation know the location of the user, or by querying the IMS network, minimizing the time to take action.
- Users that do not know the local emergency numbers can use universal identifiers in their calls [6], e.g. “urn:service:sos.ambulance”, for ambulance, leaving the P-CSCF the task to recognize it as an emergency one.

This overview is based on the existing 3GPP releases 7 and 8 specifications. Release 7 was declared frozen in TSG SA 36 in June 2007. In this release, emergency calls for IMS are supported. Within this context, 3GPP has set the requirements from both the service and regulatory points of view and are described in [8]. The emergency architecture specification is described in [9] and the corresponding protocol requirements and details are discussed in the 3GPP documents [8] and [10].

The emergency support framework for IMS is depicted in Fig. 2 and could be summarized in the following points (for more details, we refer to [8]):

1. Emergency IMS registration: can be used only to place emergency calls.
2. If the User Equipment (UE) has already retrieved its location information, it will include it in the initial request of the emergency call.
3. Otherwise the P-CSCF might query for the user location from the access network and refer it in the request. Then forward the request to a E-CSCF.
4. Upon receiving the emergency related SIP message by the E-CSCF, in case no location information was provided, the E-CSCF will query the Location

Retrieval Function (LRF) for the user location. The LRF may contain or interface with a Routing Determination Function (RDF), ensuring that the E-CSCF will receive the most appropriate PSAP URI. Then the emergency SIP message is forwarded further to this PSAP. The emergency support for IMS also provides a general mechanism to deal with the callback issue.

5. Depending on the user privacy, the PSAP client can extract the location from the SIP message or can get the updated one using the Le interface.
6. Prioritization of the SIP messages and of the data flow of the emergency call, performed by the P-CSCF enforce rules at the Policy and Charging Rule Function (PCRF) (Fig. 1) for both uplink and downlink of media, according to the Session Description Protocol (SDP) [7] parameters.

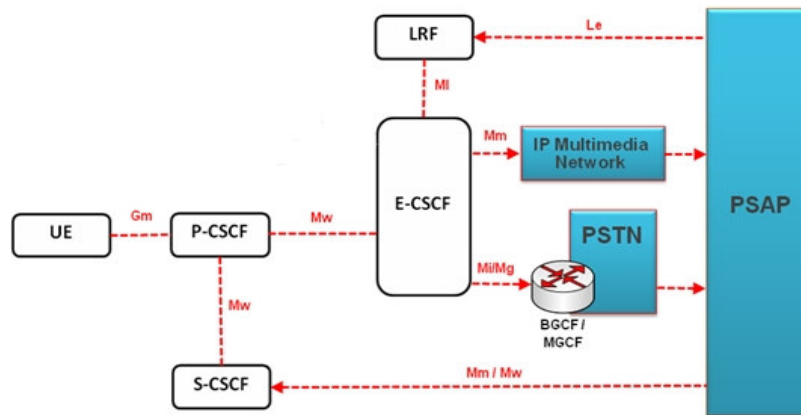


Fig 2: The emergency support framework for IMS

4 Security Issues in Emergency Services

4.1 Related Work

Like any other communications network, emergency communications are also the target of misuse and attacks. However, there are some special characteristics related to emergency services that allow the emergence of new kinds of attacks that are not visible in other communications networks. These characteristics are:

- Emergency systems are special-purpose networks with *asymmetric network behavior*: in case of a high-impact emergency event, the system will have to process a multitude of requests, while at most other times there will be very few requests.

- Emergency services are a *prioritized service*. Emergency messages have an *emergency indication* attached that guarantees to the messages to be transported immediately, and should not be delayed by other traffic.
- Emergency systems need to be *available all time* with few obstacles to the access. This means that all the relevant information should be gathered easily. On the other hand, the system should be prevented from misuse and attacks, i.e. the user might need to be authenticated. These two goals are mutually exclusive and one has to find a trade off between them.

In the literature, the work on security for emergency calls is very scarce. So far, only [4] has discussed the security threats as well as the setting of requirements to deal with them. The attacks and misuse scenarios that the mentioned characteristics can cause, described in [4], could be summarized in the following points:

- A semantic threat is a *wrong indication of the emergency location*, either by false testimony by the user or by manipulation of the calling device that automatically provides the location information (e.g. a GPS device). This can be exploited in different situations. In an emergency situation, an attacker can try to prevent help reaching its destination, by leading help resources to wrong locations.
- Prioritized traffic, especially combined with unauthenticated access is an ideal *target for misuse*. Fraudsters can try to misuse the system by using the emergency indicator into normal calls, e.g. during New Year celebrations.
- Breaching the emergency indicator system would also allow attacks on the total emergency system, e.g. a *Denial-of-Service* (DoS) attack by flooding
- An attack at the *mapping service* might rend the emergency service not operational or emergency calls might be wrongly routed, with the same effect as described in the first topic. There are basically three possibilities to attack this node: launching a DoS attack on it, gaining access to it or launching a Man-in-the-Middle attack between it and any contact point
- Emergency information is also *sensitive information*; It has to be ensured that emergency traffic can not be snooped.

Attacks can also be conducted in indirect ways. An example of how to disturb the service without actually launching an attack is to broadcast the (wrong) information that the 911 or 112 system is down and unresponsive. People will get interested or even panic and try to reach the emergency system to check if it's true. This may cause an indirect Denial-of-Service attack by hogging all available emergency lines.

RFC 5069 is without doubt a good starting point to implement built-in security mechanisms in the emergency services support for VoIP networks. However, it should be mentioned that this RFC stays a high level work and some of the scenarios described there might fail to occur in special environments like IMS.

The aim of this paper is twofold:

- Provision of more concrete attacks patterns related to RFC 5069 that might occur in the IMS emergency support framework as well as the mechanisms to prevent them
- Discussion of how the threats described in this RFC can be prevented

4.2 Some Concrete IMS Emergency Attacks

In this part, we first present the normal call pattern and then we discuss two scenarios reflecting how the emergency indicator can be abused by a malicious person to place a call to a certain destination. The first scenario shows how the *call dialog information* is misused to impersonate the PSAP, however, the second scenario discusses how the *record-route header* can be used for this purpose as well. It is also worth to mention that these scenarios can also fit in some other contexts. This can be simply achieved by impersonating an entity other than the PSAP.

Normal emergency call pattern. The P-CSCF is the IMS entity responsible for recognizing the emergency calls and prioritizing them over normal calls. To check whether an initial request is part of an emergency call, the P-CSCF compares the Request URI to the emergency dial string (e.g., 112, 911), the Emergency Universal Resource Name (URN) ([6]), and known PSAP SIP or TEL URIs[11].

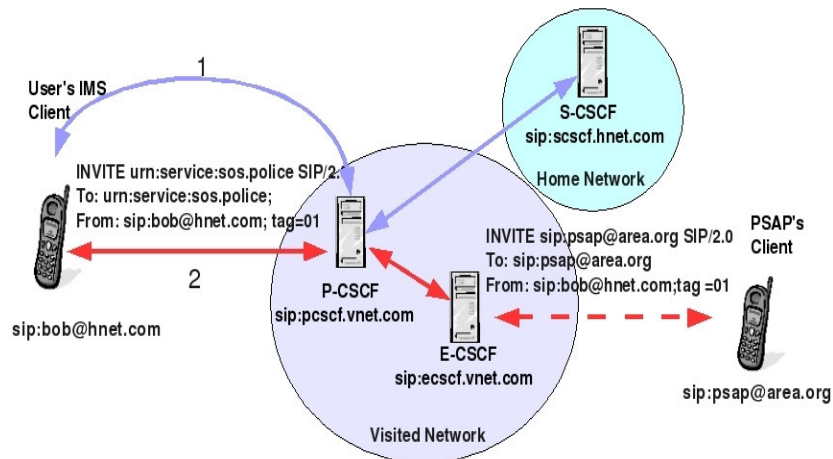


Fig 3: An example of an IMS emergency call, 1-emergency registration, 2-emergency call

The most general call flow is when the user that places the emergency call is roaming. In Fig. 3, we can see that Bob is using the SIP URI “sip:bob@hnet.com” to register and generate an emergency call destined to a general emergency service, “urn:service:sos.police”. After registration, in the 200 OK response, the UE can use the last SIP URI in the Path header as the IP address and port where the P-CSCF is expecting the UE originating requests. The INVITE request is recognized by the P-CSCF as an emergency call. The P-CSCF has to check also that the user is registered and forward the INVITE request to the E-CSCF. Here the location that Bob has provided is validated or acquired, if missing. After that the location and the type of the emergency service is mapped to the PSAP URI that should be contacted. The mapped PSAP can be IP based and registered as a SIP client, using for example the

SIP URI sip:psap@area.org. In case the PSAP is PSTN based, using a TEL URI like “tel:112” will allow to be accessible through a media gateway.

First scenario.

Attack Pattern. The emergency calls prioritization mechanism at the P-CSCF is very important to minimize the delay of the establishment of the calls and the media flow. Unfortunately, the current specifications do not provide a method for securing the interface between the P-CSCF and the E-CSCF and there are multiple use cases in which a client can use this feature for placing prioritized calls to a non-PSAP.

Let us consider that Bob, after registering with sip:bob@hnet.com wants to call Alice by pretending to call an emergency service. Suppose that Alice is using the IP 11.24.8.10 and the SIP URI sip:alice@11.24.8.10.

One way to place a malicious call is to enable Alice's client to impersonate the PSAP after an emergency session has been established. This could be possible if Bob's client would send the information about the dialog that it has gathered while the call was established. This could be done using any transport IP based protocol, to make it fast. At this stage, Alice's client is able to generate requests within the emergency dialog, by setting all the fields in the request as sent by the PSAP (Route, From, To, Contact, Call-ID) and send it to the same P-CSCF used by Bob.

In order to be able to change the audio and video settings of the call from Bob to the PSAP, Alice does not have to change the route set of the dialog, but only the SDP parameters, like the IP address, port number and codecs for audio and video data flow. For this, Alice's client can send to the P-CSCF a target refresh request, like UPDATE or re-INVITE, including its SDP parameters.

Let us consider that Alice's client will send an UPDATE request (see Fig. 4). It will be matched to the emergency dialog and forwarded based on the Route header to Bob's client. We presume that Bob's client responds with a 200 OK. If the impersonating client wants to receive the response of the UPDATE request it can add a VIA header containing its SIP URI. After the target refresh transaction has modified the SDP parameters of the session, the P-CSCF must prioritize the data flows between the two end points, considering the new SDP information. In this way a prioritized media flow between Alice and Bob can take place.

Bob's client could try to keep the session between it and the PSAP alive at the P-CSCF and E-CSCF using refresh target requests. On top of this, if the PSAP's client is using the “sip.byelless” URI media feature parameter, defined in [12], which disables a PSAP to send a release call request, and the IMS network is supporting it, there would be nothing to terminate the session, but Bob's client.

We have considered that Bob is aware of Alice's actions. But in the case that Bob is not encrypting the traffic and is using a shared environment, like an unencrypted wireless connection, someone from outside could take Alice's role or impersonate Bob and hijack or end the emergency call.

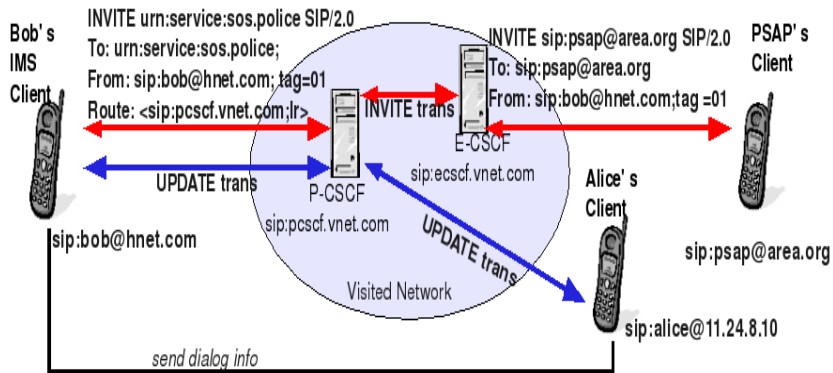


Fig 4: The dialog information misuse attack

Potential Solution. The solution to protect the IMS network from such an attack implies to secure the interface between a P-CSCF and an E-CSCF. At the P-CSCF the internal traffic should be separated from the external one, for example at the IP level. Furthermore the P-CSCF could use publicly and internally resolved IP addresses from different subnets, on separate interfaces. The E-CSCF will resolve the hostname of the P-CSCF (pcscf.vnet.com) to the internal IP address by interrogating the internal DNS server. This IP address will be used by the E-CSCF to forward the messages towards the client. The routers between the E-CSCF and the P-CSCF are part of the operator's network and not sharing the medium with any potential attacker. The client will discover and use only the external IP address of the P-CSCF. The P-CSCF will check if a SIP message has the internal or external IP address set as destination IP address and will reject the messages that are pretending to come from the PSAP but are received on the external interface. The attacker might try to guess the internal IP address, but the P-CSCF will use firewall rules to reject packages arriving at external interface and with the internal IP address as the destination IP.

Second Scenario.

Attack Pattern. Another way for Alice's client to impersonate the PSAP is to use a malicious set of Record-Route headers in the generated INVITE as the P-CSCF is not supposed to check the present of this header (see [10], subsection 5.2.6.3.3).

The preconditions model for a session establishment flow can be used in the case where one of the call parties needs a reliable transmission of provisional responses (see [13]). This mechanism can be used in case the client has to reserve resources for the call. This was mandatory in 3GPP Release 5, but 3GPP Release 6 allows session establishment without it (e.g., not both the terminals support them, or require them).

Let us suppose that this time, the attack is generated by a VoIP client, that does not support the precondition mechanism and the PSAP that is receiving the call does not require a resource allocation (see Fig. 5). The malicious Record-Route header contains Alice's SIP URI and the SIP URI that the UE is using to generate the requests.

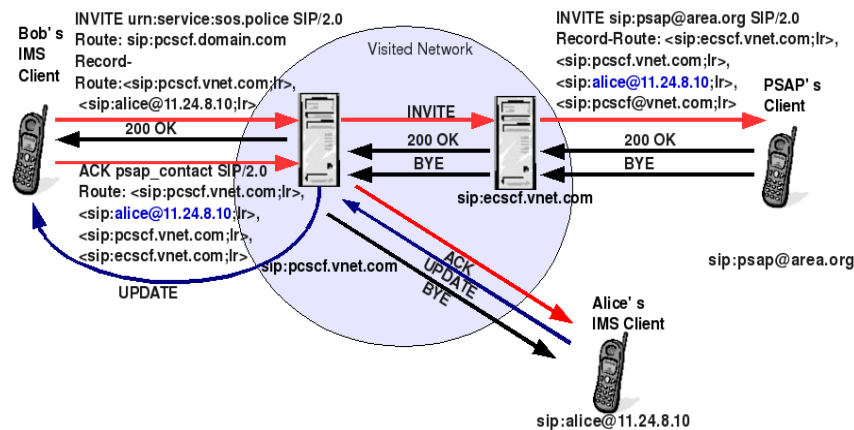


Fig 5: A scenario attack using the Record-Route header

Before forwarding the INVITE, both P-CSCF and E-CSCF, it will add their own SIP URI to the Record-Route header field, containing the port number for the subsequent requests from the PSAP and either the hostname that can be resolved to an IP address or the IP address.

The PSAP will send a 200 OK response. Before forwarding it, the P-CSCF stores the list of Record-Route header entries as the route set of the dialog.

Next, Bob's client generates an ACK request using the route set. The P-CSCF will forward the ACK to the next hop, Alice's client. After successful delivery, the P-CSCF will consider the dialog completed and the session established.

In this manner, Alice's client is able to find out all the same data that it needs to create a target refresh request (UPDATE or re-INVITE):

1. the IP address and port on which the P-CSCF is expecting to receive UE-terminating requests taken from the route set
1. the "Call-ID, From, To" header values to match the dialog
2. Contact header information of Bob's client to set as the Request-URI in the target refresh request

The next step for Alice's client is to send the target refresh request to set its SDP parameters as the called party's parameters. The response will be 200 OK and the P-CSCF will refresh the parameters by interacting with the PCRF and the media flow between Alice and Bob can start.

The conversation will last as long as the initial INVITE transaction will have not timed out, either at the E-CSCF (most probably) or at the PSAP. After the transaction times out, a BYE is generated and the dialog at the P-CSCF is destroyed and the associated resources released. The timeout interval is equal to $(64 * T1)$, and for a default value of $T1$ of 500 ms, the interval becomes 32 seconds (as stated in [14]).

Potential Solution. The P-CSCF should check if the UE has inserted a Record-Route header and its validity. In our scenario, the P-CSCF (sip:pcscf.vnet.com) was supposed to notice that the originating INVITE request contained a Record-Route

header and recognize that the Record-Route header included an entry with its SIP URI.

One way to address this attack is to enhance the P-CSCF with a mechanism to prevent the creation of erroneous route set, by checking if the Record-Route entries contain one of its IP addresses and reject the requests with an error response, for example : "403 Forbidden".

Potential solution for both scenarios. The next solutions can be applied to both scenarios and can prevent another party, other than the caller or the PSAP client, to generate and send target refresh requests to the P-CSCF that are considered to come from the PSAP client.

One solution consists of letting the P-CSCF not make visible the entire route set of the dialog to the UE that generates it. This implies that the UE knows only the next hop, the P-CSCF, and the P-CSCF is in charge of forwarding its requests to the same signaling path as the initial INVITE. The P-CSCF already has to store the route set of the dialog in order to verify if an outgoing request respects it or not. The only difference is at the forwarding time: the P-CSCF selects the next hop, in this case the E-CSCF, and forwards it the request. This method is intended to hide the internal configuration of the IMS network from any client.

Another solution would be that the P-CSCF allocates a protected port where it expects the requests from the E-CSCF. The P-CSCF is using such protected port for the messages that come from the S-CSCF and this port is communicated to the S-CSCF at the user registration, by adding a Path header including this information while forwarding the REGISTER request to the S-CSCF. As the E-CSCF is not involved in the registration, the E-CSCF is not aware of this protected port and cannot use it. The solution is that the P-CSCF adds a Path header using the same type of information (protected IP address and port) in the initial INVITE, while forwarding it to the E-CSCF. The E-CSCF should store the mentioned information and remove this header in order to keep the information only between the two entities (P-CSCF and E-CSCF). In the opposite case, the information (IP address and port) will be contained in any provisional or final response received by the caller's terminal. In this way, the E-CSCF will know at which protected port at the P-CSCF to send the next messages and the protected information will not be made available to the UE or any other party that can eavesdrop the messages in the dialog.

4.3 Security management for the IMS emergency support

To encounter the threats described in section 4.1, the emergency architecture has to be enhanced with protection mechanisms. We describe here for each threat a potential solution

General security requirements. Each security system is only as secure as its weakest link. Therefore, it has to be ensured that on the base layer, all necessary protection mechanisms are applied, including:

- Deployment and maintenance of firewalls, to allow access only to necessary services

- Protection of host systems, to protect from intrusions. Every software system has errors and these can be exploited. All security related systems need to have the latest software patches applied. Also, strong passwords need to be chosen for maintenance access
- Encrypted communication, all communication within the emergency system needs to be encrypted

Fraudulent calls that misuse the emergency identifier. It has to be ensured that only emergency calls can have the emergency identifier applied to it. It is unlikely to ensure that all access devices can be configured or secured in a way that they will not be able to misuse the emergency identifier. Instead, and based on the scenarios discussed earlier, one way to address this issue is to encrypt the communications between the emergency call parties and the IMS network, as well as within the IMS network, e.g. using Internet Protocol security (IPsec)[15]. Also the P-CSCF should be enhanced with more checking of the emergency traffic going between the callers and the PSAPs

Flooding against the mapping server or the PSAP. Denial-of-Service attacks are likely to be launched against the mapping server or the PSAP. If we take the PSAP as an example, a flooding attack can be carried out easily if the caller's device is itself the one that acquired the PSAP URI. Different proposals have been suggested to mitigate common IP-based DoS attacks [27]. However, the protection of PSAPs seems to be more complex due to their asymmetric network behavior. Traffic flashes (the generation of huge traffic volume during certain events such as earthquake or flooding) on the PSAP in case of an emergency could easily be incorrectly interpreted as a DoS attack. Dealing with such situations is complicated because on the one hand, the PSAP is not allowed to lose a single call because this might place the caller in danger, and on the other hand, it is very important that the emergency system stays available at all costs. As a consequence, we propose to enhance the PSAPs with the use of change point detection schemes such as the Cumulative Sum (CUSUM) algorithm [16]. The CUSUM can detect any sudden increase in emergency requests, which might be a DoS indicator. Once a significant increase in the volume of the emergency traffic is detected, the emergency system has to react and in an appropriate way in order to avoid dropping any emergency call as the natural consequence of this action might be the death of the caller. With other respects, we believe that a flooding attack can only be carried out with an appropriate tool, for instance an IMS client able to generate a huge number of requests. In this case, one way to react to flooding attacks is to implement a reject-second policy: Retransmission would require the attacker to keep session state information for each sent INVITE. This would increase the complexity of the attack tool and require more memory. An attacker is most likely more interested in inflicting a large processing and memory overhead on the attacked node [17]. Another option is, in case of a sudden increase of emergency calls, to route the calls to a filtering system. The latter can be an Interactive Voice Response (IVR) system, which will play an audio file such as "please wait, we will answer you call shortly" or "please press the buttons 1, 2, 3". If the emergency calls are generated by machines, they will fail to correctly handle the challenge, so the corresponding calls will be dropped. This method has certainly its drawbacks and has to take into account the various emergency communication tools that could be used by the callers in particular disabled persons. A third option is to investigate the emergency SIP

messages and look for abuse indicators, for instance, is the registration a normal registration or an emergency registration, are the location information received within the emergency calls similar or different and how big is the difference, etc.

5 IMS Emergency Support Implementation

So far, a preliminary version (ready for public testing) of the emergency enhancement related to the IMS core is available as open source software under the GNU GPL licence, see [18]). It is implemented in conformance with the 3GPP specifications TS 23.167 in the C language and ported and tested in a Linux environment.

Our IMS emergency support software is expected to be tested in public by allowing the NGN community to download the “enhanced” IMS core from the portal “www.berlios.de”, and submit it to functional, stress and performance tests. The “enhanced” IMS core can be downloaded and installed as described in [19].

The P-CSCF, I-CSCF and S-CSCF have been enhanced to be compliant to the Emergency Services specification [19], regarding emergency registration and emergency call recognition and routing. The code for the E-CSCF and the LRF entities, and testing scenarios has been also included.

The E-CSCF is a SIP statefull B2BUA that protects the identity of the PSAP. All the messages sent to the caller will contain an universal emergency identifier, based on the type of service recognized by the UE or the P-CSCF.

When sending messages to the PSAP, the E-CSCF will replace the emergency identifiers with the real PSAP SIP URI in the From or To headers. Moreover, we intend to implement the same mechanism for the Contact address as well, by statically or dynamically allocating a Contact address by the E-CSCF to PSAPs. In this way, the caller will never be able to know the SIP URI (or the associated SIP URI if a CS PSAP) or the Contact address of the PSAP, that might contain the IP address, thus being unable to directly call and attack it.

One way to implement this Contact dynamical allocation is using a pool of Contact addresses. The second way is to generate random Contact addresses.

The LRF includes a Location-to-Service Translation Protocol (LoST)[20] client, a HTTP based protocol that can be used for interrogating a LoST server about the (location, service) to URI mapping. In case of no PSAP was matched, a default local emergency call center will be used to route the call.

For testing purposes the SIPp [21] tool was used to simulate the caller and the PSAP SIP User Agents. The implementation supports both type of location format: geodetic and civic, compliant to [22] and [26]. The format of the generated messages are conform to location conveyance for SIP [14]. The testing scenarios and scripts are listed at [23].

6 IMS Emergency Support in the European Community

One of the major development goals of the emergency support for IMS is to provide the research community in general and the European in specific with a powerful and extendable open-source framework allowing the placement of daily emergency calls. This framework is being developed under the umbrella of the IST funded project PEACE [24]. To be more precise, the Fraunhofer Fokus Open IMS Core is being enhanced with some functionalities to support emergency services, for instance, emergency calls routing (E-CSCF), emergency calls recognition by the P-CSCF, and interaction with LRF.

The IMS emergency support in the context of PEACE does not stop here, however, it is also intending to address, in particular, the following issues: robustness against attacks and misuse, emergency calls prioritization, fail-over and congestion control, support of disabled persons. These issues are currently being investigated and some mechanisms to deal with them will be developed soon.

7 Conclusion

In this paper, we discussed some security issues that might be faced by the IMS emergency support. We provided two scenarios reflecting how the emergency indicator can be manipulated by an attacker to issue non-emergency calls. The first scenario shows how the *call dialog information* is misused to impersonate the PSAP, however, the second scenario discusses how the *record-route header* can be used for the same purpose. We have also suggested some solutions to the security threats related to emergency services and which were described in [4] and described our implementation.

References

1. The Internet Task Force (IETF), www.ietf.org
2. The 3rd Generation Partnership Project (3GPP), www.3gpp.org
3. Telecoms and Internet Converged Services and Protocols for Advanced Networks, (TISPAN), www.etsi.org/tispan
4. T. Taylor, et Al, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008, <http://www.ietf.org/rfc/rfc5069.txt>
5. M.Poikselkae et Al, "The IMS: IP Multimedia Concepts and Services in the Mobile Domain", Edition Wiley 2005
6. H. Schulzrinne, "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, IETF January 2008, <http://www.ietf.org/rfc/rfc5031.txt>
7. M. Handley, V. Jacobson, "SDP: Session Description Protocol", RFC 2327, IETF April 1999, <http://www.ietf.org/rfc/rfc2327.txt>
8. "Service aspects; Service principles", TS 22.101, 3GPP, <http://www.3gpp.org/ftp/Specs/html-info/22101.htm>
9. "IP Multimedia Subsystem (IMS) emergency sessions", TS 23.167, 3GPP, <http://www.3gpp.org/ftp/Specs/html-info/23167.htm>

10. "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", TS 24.229, 3GPP, <http://www.3gpp.org/ftp/Specs/html-info/24229.htm>
11. H. Schulzrinne, "The tel URI for Telephone Numbers", RFC 3966, IETF, December 2004, <http://www.rfc-editor.org/rfc/rfc3966.txt>.
12. J. Rosenberg, H. Schulzrinne, "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)" RFC 4235, IETF, <http://www.rfc-editor.org/rfc/rfc4235.txt>
13. J. Rosenberg, et Al, "Reliability of Provisional Responses in the Session Initiation Protocol", RFC 3262, June 2002, <http://www.ietf.org/rfc/rfc3262.txt>
14. J. Rosenberg, H. Schulzrinne, et Al, "SIP: Session Initiation Protocol", RFC 3261, June 2002, <http://www.ietf.org/rfc/rfc3261.txt>
15. Kent, S., K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, IETF, December 2005, <http://tools.ietf.org/html/rfc4301>
16. Y. Rebahi, "Change-Point Detection for Voice over IP Denial of Service Attacks", in the Proc of the 15. ITG/GI - Fachtagung Kommunikation in Verteilten Systemen (KiVS), Bern, Zurich, February 2007
17. J. Fiedler, T. Kupka, S. Ehlert, T. Magedanz and D. Sisalem, "VoIP Defender: Highly Scalable SIP-based Security Architecture". In the Proc of the Principles, Systems and Applications of IP Telecommunications (ACM IPTComm 2007), New York, USA, July 2007
18. Open IMS Core Home Page, FOKUS Fraunhofer Institut, Berlin, <http://openimscore.org/>
19. Installation Guide for the Emergency Branch of the Open IMS Core, FOKUS Fraunhofer Institute, http://openimscore.org/emergency_installation_guide
20. H. Schulzrinne, et. Al, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008, <http://tools.ietf.org/html/rfc5222>
21. SIPp, link: <http://sipp.sourceforge.net>
22. J. Winterbottom, M. Thomson, H. Tschofenig, „GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", link: <http://tools.ietf.org/html/rfc5491>
23. Testing Guide for the Emergency Branch of the Open IMS Core, FOKUS Fraunhofer Institute, http://openimscore.org/emergency_testing_guide
24. The PEACE project, www.ict-peace.eu
26. J. Polk, et Al, "Location Conveyance for the Session Initiation Protocol", March 2009, <http://tools.ietf.org/html/draft-ietf-sip-location-conveyance-13>
27. T. Peng et Al, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", ACM Computing Surveys, 29(1), 2007