Protecting First-Level Responder Resources in an IP-based Emergency Services Architecture

Hannes Tschofenig*, Henning Schulzrinne‡, Murugaraj Shanmugam*, Andrew Newton§

*Siemens Networks GmbH & Co KG, (hannes.tschofenig@siemens.com, murugaraj.shanmugam@siemens.com)
†Columbia University, (hgs@cs.columbia.edu)
§SunRocket, (andy@hxr.us)

Abstract—Recently, there has been increased interest, shown by the research community and by industry fora, to enable emergency services for voice-over-IP based architectures. In order to provide emergency services functionality over the Internet, several aspects like location determination, dial string configuration, location conveyance, routing to the appropriate Public Safety Answering Point (PSAP) and security aspects have to be considered. This paper discusses security threats for the IP-based emergency architecture concentrating on denial-of-service attacks against Public Safety Answering Points (PSAPs) by using faked calls that aim to exhaust limited PSAP resources, such as the emergency personnel. We illustrate a number of different approaches that have been mentioned in the past to tackle these threats, including location signing, location-by-reference and authenticated emergency calls.

1. INTRODUCTION

Users of the legacy telephone network can summon emergency services such as ambulance, fire and police using a well-known emergency service number (e.g., 9-1-1 in North America, 112 in Europe). A key factor in the handling of such calls is the ability of the system to determine the caller’s location and to route the call to the appropriate Public Safety Answering Point (PSAP) based on that location. With the introduction of IP-based telephony and multimedia services, support for emergency calling via the Internet has to be provided as well1. However, enabling such critical public services using the Internet is challenging and requires novel techniques to accomplish an emergency call. The Internet Engineering Task Force (IETF) has identified this requirement and created a working group named as Emergency Context Resolution using Internet Technologies (ECRIT) [1]. This group has focused its work on protocols and techniques to develop a robust emergency architecture which can serve all forms of IP-based networks.

To develop a robust emergency architecture, it is important to perform a detailed security analysis [5]. This paper focuses on a subset of the entire range of security aspects, such as fraudulent usage of location information and denial-of-service vulnerabilities, relevant for an emergency architecture. Before analyzing the security aspects, this manuscript provides a high level overview of an emergency call operation and briefly discusses the architectural assumptions.

To establish an emergency call, the caller needs to acquire location information, the end systems or proxies need to identify an emergency call, marking and routing it to the proper PSAP. However, there are some variants of the basic operation based on the deployment scenarios. For instance, either an end host or a proxy might determine the end host’s location information, either the end host or a SIP [3] proxy performs the initial location-based routing (i.e., the mapping of location information and emergency service identifier to PSAP URI) and the emergency call identification (including call marking) might be be done either at the end host or at a SIP proxy [4].

An important architectural assumption for the IP-based emergency services architecture is the separation of Access Infrastructure Provider (AIP) and Application (Voice) Service Provider (VSP). Today, we can observe that network access and application layer services are typically provided by different entities. We believe that it is unlikely that this model will change in the near future.

Before we investigate the details it is important to highlight the main deployment choices:

- How is location information provided?
  It might either be known to the end host itself, due to manual configuration or Global Positioning System (GPS), or available via a third party, such as a Location Server (LS) located in the access network. Even if location information is known to the network, it might be made available to the end host. Alternatively, application layer entities, such as SIP proxies, are located in the access network or have a relationship with the access network provider in order to retrieve location information to perform emergency call routing without revealing the current location to the end host.

- Is the AIP also the VSP?
  In the Internet today these roles are typically provided by different entities. As a consequence, the VSP typically does not know the current and accurate physical location of the emergency caller without additional mechanisms.

Figure 1 describes the necessary interactions between the entities in the system.
1) Location information may be available to the end host itself (e.g., manually configured or obtained via GPS),
2) Location information may, however, also be obtained from the AIP, (e.g., LLDP-MED [16], DHCP civic location information [8], DHCP geodetic location information [7]).
3) The emergency caller may need to consult a directory to determine the PSAP that is appropriate for the location of the emergency caller considering the nature of the emergency. Such a directory will be made available with the help of the Location-to-Service Translation (LoST) protocol [10] and the envisioned architecture [11].
4) The emergency caller may get assistance from emergency call routing entities. In case of Session Initiation Protocol (SIP) [3], these entities are proxies.
5) Individual emergency call routing entities might also need to consult a directory service to determine where to route the emergency call. Again, LoST can be used by these entities.
6) The emergency call routing entities need to forward the call.
7) The emergency caller may interact directly with the PSAP without any emergency call routing entity.

The overlapping squares in Figure 1 indicate that certain functionality can be collapsed. For example, the Voice Service Provider (VSP) 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 enterprises and residential users might act as their own VSP.

This paper is organized as follows: Section II presents possible security threats for the IP emergency service architecture but mainly concentrate on the attacks that could be launched against the emergency personnel, Section III discusses several approaches to mitigate the threats and finally, Section IV concludes this paper and summarizes the research challenges.

II. IP Emergency Services Architecture Security Threats

This section discusses potential security threats for the IP based emergency architecture focusing on the attacks that may be launched against the first responders (e.g., police officers and firefighters) and call takers.

One of the main motivations of an adversary in the emergency services context is to prevent callers from utilizing emergency service support. This can be done by a variety of means, such as impersonating a PSAP or directory servers, attacking SIP signaling elements and location servers. However, there are several other potential motivations that cause concern. Attackers might also wish to learn the nature of the emergency call by eavesdropping an emergency call in order to extract information for subsequent replay attacks.

Attackers may want to modify, prevent or delay emergency calls. In some cases, this will lead the PSAP to dispatch emergency personnel to an emergency that does not exist and, hence, the personnel might not be available to other callers. It might also be possible for an attacker to impede the users from reaching an appropriate PSAP by modifying the location of an end host or the information returned from the mapping protocol. In some countries it is conceivable that regulators will not demand authentication of the emergency caller as it is true for PSTN-based emergency calls today. Furthermore, if identities can easily be crafted, then the value of emergency caller authentication might be limited. As a consequence, an attacker can forge emergency call information without being able to be traced.

Note, however, that the above-mentioned attacks are mostly targeting individual emergency callers or a very small fraction of them. If attacks are, however, launched against the mapping architecture or against PSAP entities, a larger region and a large number of potential emergency callers are affected, particularly targeting the call takers at the PSAP.

In this context, three attack models need to be considered:

- **External adversary model:** The target, e.g., an emergency caller whose location is going to be communicated, is honest and the adversary may be located between the target and the location server or between the target and the PSAP. None of the emergency service infrastructure elements act maliciously.
- **Malicious emergency infrastructure adversary model:** The emergency call routing elements, such as the location server, the LoST infrastructure or call routing elements, are malicious.
- **Malicious target adversary model:** The target itself acts maliciously. This adversary model is in the main focus of the subsequent solution approaches.

A. Location Spoofing

An adversary can provide false location information in order to fool the emergency personnel. Such an attack is particularly easy if location information is attached to the emergency call by the end host and is either not verified or cannot be verified by anyone. Only entities that are close to the caller
can verify, since the correctness of location information can only be determined by them.

The following list presents threats specific to location information handling:

- **Place Shifting**: Trudy, the adversary, pretends to be at an arbitrary location.
- **Time Shifting**: Trudy pretends to be at a location she was a while ago.
- **Location Theft**: Trudy observes Alice’s location and replays it as her own.
- **Location Swapping**: Trudy and Malory, located in different locations, can collude and swap location information and pretend to be in each other’s location.

### B. Call Identity Spoofing

If an adversary is able to make emergency calls without the need to disclose its identity (such as a SIP [3] Uniform Resource Indicator (URI)), then prank calls are more difficult to be traced. There are at least two different forms of authentication in this context; network access authentication and authentication of the emergency caller at the application layer. This differentiation is created by the split between the AIP and the VSP whereby different identities, different credentials and different business partners are used.

Trying to find an adversary that did not authenticate itself to the VSP is difficult. There is, however, at least the theoretical chance to determine the adversary if network access authentication was used. If it is never authenticated (neither to the PSAP, to the VSP nor to the AIP) then it is very difficult to trace the call back in order to make a particular entity accountable. This might, for example, be the case with an open IEEE 802.11 WLAN access point even if the owner of the access point can be determined.

### C. Denial-of-Service Attack on a PSAP

A denial-of-service attack on a PSAP, for example, might isolate the PSAP temporarily from the Internet. Typically, at least two PSAPs are responsible for a certain geographical area. Attacking them means denying the service to the entire area. Although DoS attacks can be launched to any entities in the emergency calls system, from an adversary perception, attacking the PSAP is compelling. DoS attacks might appear in many different flavors ranging from standard SYN flood to attacks where a human operator has to determine whether a call is in fact a true emergency call. In some cases emergency staff, for example police or ambulance, 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.

In an emergency services context, three types of resources may be impacted, namely

1) **PSAP network facilities**, both at the network layer and for call signaling: DoS attempts that try to consume the network resources of the PSAP can be mitigated by using standard DoS protection schemes. This threat is not specific to emergency calling.

2) **Call taker resources**: This attack aims at consuming the emergency call taker resources (who answer calls in PSAPs and dispatch first responders.) at the PSAP e.g., by flooding the PSAP with emergency requests.

3) **First responders**: This attack can be launched by sending (false) requests to a particular PSAP, forcing the PSAP to dispatch their first responders. This can be done by pretending that there is an emergency at the true location of the adversary, with the help of spoofed identities, by attaching fake location or by a combination of them. If the information provided during the call request cannot be verified then the vulnerability is real. An adversary has the possibility to attach arbitrary location information. For example, an adversary may place an emergency call with location information indicating that he or she is in Austria while being in Mexico.

### III. Solution Approaches

This section presents some solution approaches to mitigate the aforementioned threats. Several solutions have been proposed attempting to rank emergency calls according to their quality and to detect and prosecute the attacker. Now, we briefly describe the basic idea of the solution approaches and categorize them according to their functionality.

#### A. Location Signing

One way to mitigate location spoofing is to let the location server sign the location information before it is sent to the target whereby the signed location information is verified by the location recipient rather than the target. Figure 2 shows the communication model with the target requesting signed location in step (1), the location server returns it in step (2) and it is then conveyed to the location recipient in step (3). In SIP, the procedures described in [6] are applicable for location conveyance.

![Communication Model for Signed Location Information](image)

Fig. 2. Communication Model for Signed Location Information.

Allowing the target to verify the digital signature provides little value particularly in an emergency situation. Hence,
the main idea is to prevent the target from tampering with the received location information since the digital signature would otherwise become invalid. The location recipient would, however, be able to verify the location information, determine who signed it and whether it was modified while in transit.

Signing location information is, however, insufficient since it allows replay attacks. Hence, additional information has to be included together with the signed location. One obvious solution is to include a timestamp and expiration time (limiting time of validity and, thus, replay). With the external adversary model, the target itself could sign the location information with the current timestamp. With the malicious target adversary model it is, however, necessary to periodically fetch signed location information from the LS (even if the target is stationary), unless the target wants to retrieve the signed location information at call time, which is not desirable since it increases the call setup delay.

To prevent location-swapping attacks it is necessary to include some some target specific identity information. The included information depends on the purpose, namely either real-time verification by the location recipient or for the purpose of a post-mortem analysis when the location recipient wants to determine the legal entity behind the target for prosecution. A more detailed treatment is, however, outside the scope of this paper and in the latter case also applicable to a location-by-reference solution.

B. Location-by-Reference

The idea of the location-by-reference concept was developed with the need to prevent the end host from periodically querying the LS for up-to-date location information in a mobile environment. Additionally, it has been speculated that some network operators do not want to make location information freely available to the target.

Figure 3 shows the communication model with the target requesting a location reference in step (1) the location server returns the reference in step (2) and it is then conveyed to the location recipient in step (3) the location recipient needs to resolve the reference with a request in step (4) and the response in step (5) for location conveyance in SIP the procedures described in [6] are applicable.

The details for the dereferencing operations, namely steps (4) and (5), vary with the type of reference, such as a HTTP / HTTPS URI or a SIP presence URI. The latter is also called subscription URI. While a HTTP/HTTPS URI can be resolved to location information in a synchronous fashion, a SIP presence URI provides further benefits due to its asynchronous nature, using the SIP SUBSCRIBE/NOTIFY concept. Location filters [12] limit location notification to events that are of relevance to its subscriber.

The target may also act in the role of the location recipient whereby it would subscribe to its own location information. For example, the target obtains a subscription URI from the future Geopriv [2] Layer 7 Location Configuration Protocol (LCP) 2 It subscribes to the URI to obtain its current location information that serves as the input to a LoST [10] query in order to acquire the PSAP service boundary. The service boundary indicates the region where the device can move without the need to re-query since the LoST answer remains unchanged. The target may use the PSAP service boundary as a location filter at the LS. If the target moves outside a certain area, as indicated by the location filter, it will receive a notification and knows that it has to re-run LoST to obtain a new mapping and also a new service boundary.

For location-by-reference, the LS needs to maintain one or several URIs for each target, timing out these URIs after a certain amount of time. References need to expire to prevent the recipient of such a URL from being able to permanently track a host and to offer garbage collection functionality for the LS.

Off-path adversaries must be prevented from obtaining the target’s location. There are at least two approaches to provide this property: The location reference contains a randomized component that allows any holder of the reference to obtain location information. Alternatively, the reference can be public and the LS performs access control via a separate authentication mechanism, such as HTTP digest or TLS client-side authentication when resolving the reference to a location object. After authentication, the LS needs to inspect a rule set to perform authorization whereby these rules may be provided by the target.

The former alternative allows the location recipient to authenticate the location server but does not demand authentication of the location recipient towards the location server. This simplifies deployment. Authenticating the location signing

---

2 A document that provides a problem statement, requirements and design aspect are available with [9]. The usage of this Geopriv L7 LCP protocol is also relevant for the signed location information discussion since the target needs a way to interact with the LS. A few protocol proposals are available with ’HTTP Enabled Location Delivery’ (HELDD) [13], ’Retrieving End System Location’ (RELO) [15] and ’A Location Reference Event Package for the Session Initiation Protocol ’ (LocationRef) [14] but only as individual contributions rather than as an official IETF standard.
entity is insufficient and verifying that the location server is trustworthy is challenging.

When the LR fetches up-to-date location information from the LS, the LR can also be assured that the location information is fresh and not replayed.

C. Authenticated Calls

In many cases, authenticated calls, i.e., verifying the callers identity, are at least as useful as location signing since they establish accountability for later prosecution.

If most of the legitimate calls are authenticated in some way (this is possible with botnets, which can use real identity and location of the caller), then it is possible, under attack conditions only, to give “dubious” calls lower priority or to have them go through some sort of “Turing” tests (However, such tests are not exactly helpful when a caller is under stress; speak many different languages etc). As an example, PSAP operators do not want to reject emergency calls but if the alternative is wasting 90 percent of the resources on bogus calls (and thus leaving many legitimate callers stranded) and not handling the unlucky unauthenticated, the expected outcome is better if one can separate. This is the standard “triage” model used in emergency medicine.

If somebody places a signed (known-third-party VSP-authenticated) call, there is, at least, the possibility of catching a malicious caller and the number of such calls is limited. Thus, there are only legitimate calls left

- that use end system location determination (e.g., GPS, manual configuration), and
- that have no (known) VSP, and
- that are not signed in some other way.

For example, for emergency purposes, authentication could be based on public key certificates that independent from any subscription of the the target to the VSP or ISP. This solution could be deployed with separate certificates offered to VoIP devices in order to place emergency calls. When the location information that is sent to the end host is corrupted, for example when provided by the location server, then it might not be possible to make the LS operator responsible.

D. Evaluation

This section discusses the attack model and describes some possible countermeasures in detail. Furthermore it provides an evaluation of the possible solution approaches with respect to the attack model. With the external adversary model we assumed that the adversary is located either between the LS and the target or between the target and the location recipient. By securing the communication between the LS and the target and between the target and the location recipient, the threats such as eavesdropping and replaying the location information can be mitigated.

To mitigate the malicious emergency infrastructure attack model, i.e., the infrastructural elements such as LoST server, call routing elements are malicious, the target must be able to authenticate the infrastructural elements. For instance, the target must authenticate the LoST server, e.g., using TLS, before requesting the mapping information.

The main threat model, we consider in this paper, is the malicious target adversary model, where the target itself launches the attack against the emergency architecture. In place shifting cases, the target attaches some arbitrary location information to fool the emergency responder. This is possible due to the fact that the attached location information is never authenticated or verified. To avoid such attacks, it is compelling to use Signed Location (SLoc) information (i.e., performing a digital signature over the location information by a LS) and let the final location recipient verify the authenticity of the provided information. This will restrict the attacker from attaching or modifying the signed location information. However, the signed location information does not prevent the attacker to use it over an extended period of time. This form of attack is called Time shifting and to avoid such threats, it is obvious to include the expiry time (SLoc+Time) of the provided location. This time window will further restrict attacker not to use the same location information from a different place at a different time.

By including the validity time and by adding a signature, one can prevent certain attacks but does not eliminate all threats. This is because that the attacker is still able to use the signed location with validity information within the specified time window to launch false requests. Swapping location objects is also possible. This motivates adding also including target and end user-specific identifier into the signed location object.

The purpose of these identifiers is two-fold: They offer the ability to trace back an adversary by giving the PSAP provider the ability to determine the access provider and in a second step the user that authenticated to the access network (potentially involving another indirection step in case of roaming). It does not help in case of unauthenticated network access and does not offer real-time verification steps by the PSAP operator at the time of receiving the emergency call. For a real-time check it is necessary to tie the emergency call to the content of the signed location object via identity information, such as the one used for SIP end-to-end authentication. This type of identity has to be non-spoofable but the end user should not loose its privacy protection against the access network in case of a non-emergency situation. Since the authors try to depict the high-level ideas rather than describing the details of each proposal we have to omit a detailed analysis of these types of identities.

The location-by-reference (LbyR) concept does not allow the target to modify the location information. However, the LbyR concept is also vulnerable to attacks, such as location swapping, and requires a treatment similar to location-by-value.

In case of authenticated calls at the VSP level the chance to trace back the bogus caller for later prosecution is provided even though the location information itself is unprotected. Table 1 shows that the location-by-value and the location-by-reference mechanism provide the same security protection when appropriately enhanced. This allows to evaluate the quality of the emergency call in real-time by the PSAP operator. Since emergency calls are not rejected even though they appear suspicious, the provided benefit is largely for ranking calls.
An authenticated emergency call does not provide protection against the listed attacks but offers the ability to reveal the identify of the adversary for later prosecution.

IV. SUMMARY AND RESEARCH CHALLENGE

The ability to access “life-critical” emergency services, such as police or ambulance, is an important and inherent feature of the PSTN. On the other hand, VoIP is an emerging technology that enables its users to place and receive calls via Internet. For the VoIP end customer there is the expectation that emergency services are available as they are with the PSTN. However, enabling such services is not a trivial task and requires to re-evaluate the design choices made for the traditional emergency architecture. For example, the location concept and security aspects in an IP-based emergency environment pose new design constraints.

This paper points out and discusses some potential security threats in the IP-based emergency architecture that may well be exploited by the attackers to damage the emergency service system. Therefore, we presented attack scenarios that could lead to DoS on the emergency personnel itself, i.e., exhausting the limited (human) PSAP resources by directing the first responder to a wrong location or a non-existing incident. We have discussed some possible solutions that aim to deal with the threat.

Unfortunately, it is not entirely clear how to evaluate the trade offs between the proposed mechanisms and whether the solutions will actually improve the robustness and efficiency of the overall emergency services architecture. For example, using the signed location concept addresses some threats but requires changes within the emergency service infrastructure. Hence, this paper aims to stimulate further research in this area to provide input to the current standardization work that is being done in the IETF.

ACKNOWLEDGMENTS

We would like to thank the members of the IETF ECRIT and the IETF GEOPRIV working group for their input to the discussions related to this topic.

REFERENCES