ECRIT
Internet-Draft
Expires: September 21, 2006

T. Taylor
(Editor) Nortel
H. Tschofenig
Siemens
H. Schulzrinne
Columbia U.
M. Shanmugam
Siemens
March 20, 2006

Security Threats and Requirements for Emergency Call Marking and Mapping

draft-ietf-ecrit-security-threats-00.txt

Status of this Memo

Copyright Notice

Abstract

This document reviews the security threats associated with the two current work items of the ECRIT Working Group. The first is the marking of signalling messages to indicate that they are related to

an emergency. The second is the process of mapping from locations to Universal Resource Identifiers (URIs) pointing to Public Safety Answering Points (PSAPs). This mapping occurs as part of the process of routing emergency calls through the IP network. Based on the threats, this document establishes a set of security requirements for the the mapping protocol and for the handling of emergency-marked calls.

Table of Contents

1. Introduction

Legacy telephone network users can summon help for emergency services such as ambulance, fire and police using a well known number (e.g., 911 in North America, 112 in Europe). A key factor in the handling of such calls is the ability of the system to determine caller 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 also has to be provided. As one of the steps to achieve this, an emergency marker must be defined that can be attached to call signalling to indicate that the call relates to an emergency. In addition, a protocol must be developed allowing a client entity to submit a location and receive a URI pointing to the applicable PSAP for that location.

Attacks against the PSTN (most often focusing on free calling) have taken place for decades. The Internet is seen as an even more hostile environment. Thus it is important to understand the types of attacks that might be mounted against the infrastructure providing emergency services, and to develop security mechanisms to counter those attacks. In view of the mandate of the ECRIT Working Group, the present document restricts itself to attacks on the mapping of locations to PSAP URIs and attacks based on emergency marking.

This document is organized as follows: Section 2 describes basic terminology. Section 3 briefly describes how emergency marking and mapping fit within the process of routing emergency calls. Section 4 describes some motivations of attackers in the context of ECRIT, Section 5 describes and illustrates the attacks that might be used, and Section 6 lists the security-related requirements that must be met if these attacks are to be mitigated.

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], with the qualification that unless otherwise stated they apply to the design of the mapping protocol, not its implementation or application.

The terms call taker, mapping service, emergency caller, emergency identifier, mapping, mapping client, mapping server, mapping protocol, and Public Safety Answering Point (PSAP) are taken from [I-D.ecrit-requirements].

The term "location information" is taken from RFC 3693 [RFC3693].

The term "emergency caller's device" designates the IP host closest to the emergency caller in the signalling path between the emergency caller and the PSAP. Examples include an IP phone running SIP, H.323, or a proprietary signalling protocol, a PC running a soft client, or an analogue terminal adapter or a residential gateway controlled by a softswitch.

3. Marking, mapping, and the emergency call routing process

The ECRIT Working Group has two work items relating to the routing of emergency calls to their proper destination. The first is to enable entities along the signalling path to recognize that a particular signalling message is associated with an emergency call. The ECRIT Working Group is defining content that can be added to the signalling messages, an emergency identifier, for this purpose. Signalling containing the emergency identifier may be given priority treatment, special processing, and/or special routing.

The first goal of emergency call routing is to ensure that any emergency call is routed to a PSAP. Preferably the call is routed to the PSAP responsible for the caller's location, since misrouting consumes valuable time while the call taker locates and forwards the call to the right PSAP. As described in [I-D.ecrit-requirements], mapping, the second ECRIT work item, is part of the process of achieving this preferable outcome.

In brief, mapping involves a mapping client, a mapping server, and the protocol that passes between them. The protocol allows the client to pass location information to the mapping server and to receive back a URI which can be used to direct call signalling to a PSAP.

Since mapping requires location information for input, when and where the location information is acquired imposes constraints upon when mapping can be done and which devices can act as mapping clients. The key distinction in "when" is before the emergency or during the emergency. The key distinction in "where" is at the emergency caller's device or at another device in the signalling path between the emergency caller and the PSAP. The device that acquires the location information can be the mapping client, and so can any device downstream of that point. It is even possible for a PSAP itself to initiate mapping, to determine whether an arriving call should be handled by a call taker at that PSAP or should be proxied to another PSAP.

4. Objectives of attackers

Attackers may direct their efforts either against a portion of the emergency response system or against an individual. Attacks against the emergency response system have three possible objectives:

- to deny system services to all users in a given area. The motivation may range from thoughtless vandalism, to wide-scale criminality, to terrorism. One interesting variant on this motivation is the case where a victim of a large emergency hopes to gain faster service by blocking others' competing calls for help.

- attacks by the caller to gain fraudulent use of services, by using an emergency identifier to bypass normal authentication, authorization, and accounting procedures.

- to divert emergency responders to non-emergency sites. No attacks affecting the ECRIT Working Group's decisions on the emergency identifier and mapping protocol have been identified that achieve this objective

Attacks against an individual fall into two classes:

- attacks to prevent an individual from receiving aid;

- attacks to gain information about an emergency that can be applied either against an individual involved in that emergency or to the profit of the attacker;

5. Potential attacks

5.1. Attacks involving the emergency identifier

The main attack possibility involving the emergency identifier is to use it to bypass normal procedures in order to achieve fraudulent use of services. An attack of this sort is possible only if the following conditions are true:

a. The attacker is the emergency caller.

b. The call routing system assumes that the emergency caller's device addresses emergency calls using the result of mapping based on the caller's location.

c. The call enters the domain of a service provider, which accepts it without applying normal procedures for authentication and authorization because the signalling carries the emergency identifier.

d. The service provider routes it according to the called address (e.g., SIP Request-URI), without verifying that this is the address of a PSAP (noting that a URI by itself does not indicate the nature of the entity it is pointing to).

If these conditions are satisfied, the attacker can bypass normal ASP/VSP authorization procedures for arbitrary destinations, simply by reprogramming the emergency caller's device to add the emergency identifier to non-emergency call signalling. Most probably in this case, the call signalling will not include any location information.

An attacker wishing to disrupt the emergency call routing system may use a similar technique to target components of that system for a denial of service attack. The attacker will find this attractive to reach components that handle emergency calls only. Flooding attacks are the most likely application of the technique, but it may also be used to identify target components for other attacks by analyzing the content of responses to the original signalling messages.

5.2. Attacks against or using the mapping process

This section describes classes of attacks involving the mapping process that could be used to achieve the attacker goals described in Section 4.

5.2.1. Attacks against the emergency response system

This section considers attacks intended to reduce the effectiveness

of the emergency response system for all callers in a given area. If the mapping operation is disabled, the immediate effect is to increase the probability that emergency calls are routed to the wrong PSAP. This has a double consequence: emergency response to the affected calls is delayed, and PSAP call taker resources outside the immediate area of the emergency are consumed due to the extra effort required to redirect the calls. Alternatively, attacks that cause the client to receive a URI that does not lead to a PSAP have the immediate effect of causing emergency calls to fail.

Three basic attacks on the mapping process can be identified: denial of service, impersonation of the mapping server, or corruption of the mapping database. Denial of service in turn can be achieved in several ways:

- by a flooding attack on the mapping server;
- by taking control of the mapping server and either preventing it from responding or causing it send incorrect responses; or
- by taking control of a router through which the mapping queries and responses pass and using that control to block them. An adversary may also attempt to modify the mapping protocol signaling messages. Additionally, it might be possible to replay past communication exchanges to fool an emergency caller by returning incorrect results.

In an impersonation attack, the attacker induces the mapping client to direct its queries to a host under the attacker's control rather than the real mapping server. Impersonation itself is an issue for mapping server discovery rather than for the mapping protocol directly. However, the mapping protocol may help to protect against acceptance of responses from an impersonating entity.

Corruption of the mapping database cannot be mitigated directly by mapping protocol design. The mapping protocol may have a role to play in analysis of which records have been corrupted, once that corruption has been detected.

Beyond these attacks on the mapping operation itself, it is possible to use mapping to attack other entities. One possibility is that mapping clients are misled into sending mapping queries to the target of the attack instead of the mapping server. Prevention of such an attack is an operational issue rather than one of protocol design. The other possible attack is one where the the mapping server is tricked into sending responses to the target of the attack through spoofing of the source address in the query.

5.2.2. Attacks to prevent a specific individual from receiving aid

If an attacker wishes to deny emergency service to a specific individual the mass attacks described in Section 5.2.1 will obviously work provided that the target individual is within the affected population. Except for the flooding attack on the mapping server, the attacker can in theory limit these attacks to the target, but this requires extra effort that the attacker is unlikely to expend. It is more likely, if the attacker is using a mass attack but does not wish it to have too broad an effect, that it is used for a carefully limited period of time.

If the attacker wants to be selective, however, it may make more sense to attack the mapping client rather than the mapping server. This is particularly so if the mapping client is the emergency caller's device. The choices available to the attacker are similar to those for denial of service on the server side:

- a flooding attack on the mapping client;
- taking control of a router through which the mapping queries and responses pass and using that control to block or modify them.

Taking control of the mapping client is also a logical possibility, but raises no issues for the mapping protocol.

5.2.3. Attacks to gain information about an emergency

This section discusses attacks used to gain information about an emergency. The attacker may be seeking the location of the caller (e.g., to effect a criminal attack). The attacker may be seeking information that could be used to link an individual (the caller or someone else involved in the emergency) with embarrassing information related to the emergency (e.g., "Who did the police take away just now?"). Finally, the attacker could be seeking to profit from the emergency, perhaps by offering his or her services (e.g., news reporter, lawyer aggressively seeking new business).

The primary information that interceptions of mapping requests and responses will reveal are a location, a URI identifying a PSAP, and the addresses of the mapping client and server. The location information can be directly useful to an attacker if the attacker has high assurance that the observed query is related to an emergency involving the target. The other pieces of information may provide the basis for further attacks on emergency call routing, but because of the time factor, are unlikely to be applicable to the routing of the current call. However, if the mapping client is the emergency caller's device, the attacker may gain information that allows for

interference with the call after it has been set up or interception of the media stream between the caller and the PSAP.

6. Security requirements relating to ECRIT work items

This section describes the security requirements which must be fulfilled to prevent or reduce the effectiveness of the attacks described in Section 5. The requirements are presented in the same order as the attacks.

From Section 5.1:

Attack: fraudulent calls.

Requirement: for calls which meet conditions a-c of Section 5.1, the ASP/VSP call routing entity MUST verify that the destination address (e.g., SIP Request-URI) presented in the call signalling is that of a PSAP.

Attack: use of emergency identifier to probe in order to identify emergency call routing entities.

Requirement: topology hiding SHOULD be applied to call signalling returned to the emergency caller, so that the identity of intermediate routing entities is not disclosed. The obvious exception is where these entities are already visible to the caller. Note that there is little point in hiding the PSAP itself.

From Section 5.2.1:

Attack: flooding attack on the mapping client, mapping server, or a third entity.

Requirement: The mapping protocol MUST NOT create new opportunities for flooding attacks, including amplification attacks.

Attack: insertion of interfering messages.

Requirement: The protocol MUST permit the mapping client to verify that the response it receives is responding to the query it sent out.

Attack: man-in-the-middle alteration of messages.

Requirement: The protocol MUST maintain request and response integrity.

Attack: impersonation of the mapping server.

Requirement: the security considerations for any discussion of mapping server discovery MUST address measures to prevent impersonation of the mapping server.

Requirement: the protocol MUST permit the mapping client to authenticate the source of mapping responses.

Attack: corruption of the mapping database.

Requirement: the security considerations for the mapping protocol MUST address measures to prevent database corruption by an attacker.

Requirement: to provide an audit trail, the protocol SHOULD allow the inclusion of an identifier in its response that indicates which database records were used in preparing the response. This identifier SHOULD be encrypted along with randomizing information such as date/time, to minimize the information provided to an attacker in mapping responses.

From Section 5.2.2: no new requirements.

From Section 5.2.3:

Attack: snooping of location and other information.

Requirement: the protocol MUST maintain confidentiality of the request and response.

7. Security Considerations

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

8. Acknowledgements

The writing of this document has been a task made difficult by the temptation to consider the security concerns of the entire personal emergency calling system, not just the specific pieces of work within the scope of the ECRIT Working Group. Hannes Tschofenig performed the initial security analysis for ECRIT, but it has been shaped since then by the comments and judgement of the ECRIT WG at large. At an earlier stage in the evolution of this document, Stephen Kent of the Security Directorate was asked to review it and provided extensive comments which led to a complete rewriting of it. Brian Rosen, Roger Marshall, Andrew Newton, and most recently, Spencer Dawkins have also provided detailed reviews of this document at various stages. The authors thank them.

9. IANA Considerations

This document does not require actions by the IANA.

10. References

10.1. Normative References

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

[RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

10.2. Informative References

[I-D.ecrit-requirements] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", February 2006.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

Authors' Addresses

Tom Taylor
Nortel
1852 Lorraine Ave
Ottawa, Ontario K1H 6Z8
Canada

Email: taylor@nortel.com

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

Email: murugaraj.shanmugam@siemens.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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