SIPPING
Internet-Draft
Intended status: Informational
Expires: December 16, 2007

H. Tschofenig, Ed.
Nokia Siemens Networks
G. Dawirs
University of Namur
T. Froment
Alcatel-Lucent
D. Wing
Cisco
H. Schulzrinne
Columbia University
June 14, 2007

Requirements for Authorization Policies to tackle Spam for Internet Telephony and Unwanted Traffic
draft-froment-sipping-spit-requirements-00.txt

Status of this Memo

Copyright Notice

Abstract

Spam over Internet Telephony (SPIT) is one of the foreseen future forms of spamming that SIP open-wide networks may have to handle. SPIT also has more impact on users than email spam since it is more intrusive. Email as a store-and-forward communication mechanism allows for several filtering mechanisms to be applied to the full content before being presented to the user. Session Initiation Protocol (SIP) interaction is, in contrast, real-time communication and therefore does not provide much information prior to the transmission of the content, making it both harder to filter and more annoying to users. The responsibility for filtering, blocking calls, or taking any other preventive action can belong to different elements in the call flow and may depend on various factors.

This document discusses the requirements to define authorization policies that should allow end users or other parties to setup anti-SPIT policies for triggering these actions. These policies typically match a particular SIP communication pattern based on a number of attributes. The range of attributes includes information provided, for example, by the SIP protocol itself, by the SIP identity mechanism, by information carried within SAML assertions, reputation systems of social networks and other extensions.

Table of Contents

1. Introduction

The problem of SPIT is an important challenge and it appears that a combination of several techniques is desirable to provide a framework to deal with it.

One important building block is to provide a mechanism to instruct a trusted SIP proxy or any other SIP element to influence message handling of incoming requests according to policies. Different entities, such as end users, parents on behalf of their kids or system administrators, might create and modify authorization policies.

Some attributes in an incoming message play a more important role than others. For example, applying authorization policies based on the authenticated identity, see [RFC4474], is an effective way to make decisions regarding unwanted traffic in many cases.

This document identifies requirements for authorization policies when used to influence message handling for unwanted communicaion attempts.

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 RFC 2119 [RFC2119], with the important qualification that, unless otherwise stated, these terms apply to the design of the authorization policies, not its implementation or application.

The term 'Rule Maker' is defined in RFC 3693 [RFC3693].

3. Requirements

This section lists the requirements categorized according to their applicability for the "conditions", "actions" and "transformation" parts of authorization policies. Furthermore, we describe requirements that are more generic in nature and apply to the entire rule set.

3.1. Conditions

The first set of requirements refer to identity related information.

Req-C 1: Policies MUST allow conditions to express single authenticated identities.

Req-C 2: Policies MUST allow filtering based on the domain part of the identity.

Req-C 3: Policies MUST support the differentiation between authenticated and unauthenticated identities.

Req-C 4: Policies MUST be able to express expections within a group of users/domain.

Message handling might be different depending on the content of the SIP message header fields.

Req-C 5: Policies SHOULD allow conditions to refer to the "destination" (which corresponds to the "Request-URI") and "original-destination" (which corresponds to the "To" header).

Req-C 6: Policies SHOULD allow conditions to refer to the method invoked by the caller (e.g., INVITE, REFER, MESSAGE). Motivation: Some SIP methods are more intrusive than others (the default applicative behaviour when SIP MESSAGEs are received is often to pop-up the message on the UAS side), adopting a different filtering policy depending of the method invoked will enhance the user's protection.

Req-C 7: Policies SHOULD allow Rule Makers to take actions on messages that are marked as Spam.

Note that such a condition element should be seen in context of the authenticated domain or or otherwise protected information to avoid security vulnerabilities.

[Editor's Note: Should we allow message handling based on the

existence or non-existence of certain SDP / SIP content, such as specific mime types? For example, is a "exists" test useful that returns true if the headers listed in the argument exist within the message. Furthermore, do we need test operators (such as "allof" and "anyof", which implement logical "and" and logical "or", respectively)?

Message handling might be different based on time.

Req-C 7: Policies SHOULD allow conditions that refer to the reception date, time or period of time of the incoming request.

Message handling might be different based on the language.

Req-C 8: Policies SHOULD allow to make decisions based on the languages in which the originator of the call wishes to communicate.

Message handling might be different based on the SIP resource priority fields, on emergency service related messages or more generic forms of indicating the type of service.

Req-C 9: Policies MAY allow to make decisions based on the presence of SIP Resouce Priority headers, as described in [RFC4412].

Req-C 10: Policies SHOULD allow to make decisions based on the messages marked as emergency calls indicated in [I-D.ietf-ecrit-service-urn].

Req-C 11: Policies MAY allow to make decisions based on service identification fields, see [I-D.rosenberg-sipping-service-identification].

3.2. Actions

Req-A 1: Policies SHOULD allow messages to get "blocked", i.e., to stop forwarding the request and to return an answer with a ``403 Forbidden''

Req-A 2: Policies SHOULD allow messages to get "politely blocked", i.e., to drop the request without returning an answer.

Req-A 2: Policies SHOULD allow messages to get "marked", i.e., to forward the request and mark it as "potential Spam" for filtering at the end point or at subsequent entities along the signaling path.

Req-A 3: Policies SHOULD allow messages to be "allowed", i.e., to

forward this message.

Req-A 4: Policies MUST allow messages to be "redirected" to, for example, voicemail or to a different device in the possession of the user.

Req-A 5: Policies MUST allow the ability to execute other SPIT prevention procedures, such as computational puzzles [I-D.jennings-sip-hashcash] or the consent framework" [I-D.ietf-sip-consent-framework]. Ideally, a specification developing a SPIT prevention mechanism SHOULD provide information on how they can be incorporated into the authorization policy framework.

> As an example, for a statistical analysis tool a URI is defined. The algorithms itself do not need to be standardized and hence the impact for authorization policies is mainly the ability to allow a Rule Maker to enable or to disable the usage of these statistical techniques for SPIT filtering and potentially to map the output of the analysis process to value range from 0 (i.e., the message is not classified as Spam) and 100 (i.e., the message was classified as as Spam). A Rule Maker may decide the appropriate action on the message depending on the determined SPIT probability.

Req-A 6: Policies MAY allow an e-mail (or SMS, MMS) to be sent to the user about the actions taken due to a specific call attempt.

3.3. Transformations

Req-T 1: Policies SHOULD allow SIP messages to be marked with a certain SPIT probability in case SPIT detection and policy enforcement is excecuted on different entities. For example, a network element might run a statistical SPIT detection tool but the authorization policies are executed on a different entity, such as the end host. Note that it needs to be ensured that an adversary is not able to set the SPIT probabity values since otherwise the authorization policies that rely on such information are misguided.

3.4. Generic Requirements

Req-G 1: It SHOULD be possible to allow a hierarchy of authorization policies to be used.

Req-G 2: It MUST be possible for a client to learn the supported authorization policy capabilities implemented by the server.

Req-G 3: Policies MUST be extensible and these extensions MUST exist within a different namespace. Furthermore, a published schema and the namespace for elements defined within it MUST NOT be altered by future specifications.

Req-G 4: The policies MUST provide a mandatory-to-implement conflict resolution mechanism.

4. IANA Considerations

This document does not require actions by IANA.

5. Security Considerations

This document describes the requirements for elements contained in the authorization policies that allow communication attempts to be treated differently based on the content of the message, time-of-day, context of the user, reputation of the sending party, and many other factors.

The security concerns are related to the ability of certain entities to create, update and delete authorization policies. If an unauthorized entity is allowed to modify policies (and to distribute them to other domains) then a denial of service attack is the consequence with impact for more than a single end point. These security aspects are, however, not subject of this document.

6. Acknowledgements

The content of this document is inspired by the work of CPL [RFC3880], SIEVE [I-D.ietf-sieve-3028bis], Common Policy [RFC4745] and Presence Authorization Policy [I-D.ietf-simple-presence-rules]. We would like to thank the authors of these documents for their work.

7. References

7.1. Normative References

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

7.2. References

[I-D.ietf-ecrit-service-urn]
Schulzrinne, H., "A Uniform Resource Name (URN) for Services", draft-ietf-ecrit-service-urn-06 (work in progress), March 2007.

[I-D.ietf-sieve-3028bis]
Showalter, T. and P. Guenther, "Sieve: An Email Filtering Language", draft-ietf-sieve-3028bis-12 (work in progress), February 2007.

[I-D.ietf-simple-presence-rules]
Rosenberg, J., "Presence Authorization Rules", draft-ietf-simple-presence-rules-09 (work in progress), March 2007.

[I-D.ietf-sip-consent-framework]
Rosenberg, J., "A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP)", draft-ietf-sip-consent-framework-01 (work in progress), November 2006.

[I-D.jennings-sip-hashcash]
Jennings, C., "Computational Puzzles for SPAM Reduction in SIP", draft-jennings-sip-hashcash-05 (work in progress), June 2007.

[I-D.rosenberg-sipping-service-identification]
Rosenberg, J., "Identification of Communications Services in the Session Initiation Protocol (SIP)", draft-rosenberg-sipping-service-identification-02 (work in progress), May 2007.

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

[RFC3880] Lennox, J., Wu, X., and H. Schulzrinne, "Call Processing Language (CPL): A Language for User Control of Internet Telephony Services", RFC 3880, October 2004.

[RFC4412] Schulzrinne, H. and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)", RFC 4412, February 2006.

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

[RFC4745] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", RFC 4745,

February 2007.

Authors' Addresses

Hannes Tschofenig (editor)
Nokia Siemens Networks

Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.com

Geoffrey Dawirs
University of Namur
21, rue Grandgagnage
Namur B-5000
Belgique

Email: gdawirs@gdawirs.be

Thomas Froment
Alcatel-Lucent
Route de Villejust
Nozay, Paris 91620
France

Email: Thomas.Froment@alcatel-lucent.fr

Dan Wing
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: dwing@cisco.com

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

Phone: +1 212 939 7004
Email: hgs@cs.columbia.edu
URI: http://www.cs.columbia.edu

Full Copyright Statement

Intellectual Property

Acknowledgment

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