Authorization Policies for Preventing SPIT

draft-froment-sipping-spit-authz-policies-00.txt

Status of this Memo

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

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

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

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on August 24, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

SPAM, defined as sending unsolicited messages to someone in bulk, might be a problem on SIP open-wide deployed networks. The responsibility for filtering or blocking calls can belong to different elements in the call flow and may depend on various factors. This document discusses mechanisms to establish policies to
react on potentially unwanted communication attempts.

These policies match a particular SIP communication pattern based on a number of attributes. The range of attributes includes information provided, for example, by the Session Initiation Protocol, SIP identity mechanism, SIP-SAML and SPIT-SAML.

An important topic for investigation is to decide whether the problem is worth analyzing, the choice of a policy language for describing authorization policies and to provide a mechanisms to create and modify authorization policies that are stored in XML documents.

Table of Contents

1. Introduction ......................................................... 3
2. Terminology .......................................................... 4
3. Framework ............................................................ 5
4. Requirements .......................................................... 8
5. Discussion and Open Issues ......................................... 10
  5.1. Extending Geopriv Authorization Policies ....................... 10
  5.2. Hierarchical Authorization Policy Documents ................... 10
6. IANA Considerations .................................................. 11
7. Security Considerations .............................................. 12
8. Acknowledgements .................................................... 13
9. References ............................................................. 14
  9.1. Normative References ............................................. 14
  9.2. Informative References .......................................... 14
Authors’ Addresses ..................................................... 16
Intellectual Property and Copyright Statements ....................... 17
1. Introduction

The problem of SPAM for VoIP seems to become a very big challenge and only "the combination of several techniques can provide a framework for dealing with spam in SIP" (as stated in [I-D.jennings-sip-hashcash]).

One important building block is to have a mechanism to offer a mechanism to instruct some entities in the network to "filter" incoming requests according to user or to network-wide policies. Different entities, such as users or system administrators, might create and modify authorization policies and might even share these policies between domains.

Some attributes in a SIP communication play a more important role than others. For example, there is reason to believe that applying authorization policies based on the authenticated policies is an effective way to accept a communication attempt in order to compat SPIT. The same is true for policies that are applied to deployment friendlier SIP security solutions, such as the SIP identity mechanism [I-D.ietf-sip-identity].
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].
3. Framework

The framework of the discussed anti-SPIT authorization policies looks as follows:

![Diagram of framework]

Authorization policies can be applied at the end host and/or by intermediaries. The rule maker might be an user that owns the end device, a VoIP service provider, a person with a relationship to the end user (e.g., the parents of a child using a mobile phone). The subsequent text lists a few use cases.

The first use case that can be imagined is the case of a user that asks its outbound proxy to offer protection of requests from a particular SIP UA. He can create an authorization policy rule and upload it to the SIP proxy within its own domain. Requests coming from this SIP URI will then be blocked or treated differently.
Supposing "B@otherdomain.com" has added an authorization rule blocking request coming from domain example.com. Here is a potential message sequence:

```
A@example.com       Proxy          Proxy      B@otherdomain.com
@example.com  @otherdomain.com

| INVITE          |               |                |
| B@otherdomain.com               |                |
-------------------------->  INVITE
| B@otherdomain.com               |                |
-------------------------->  403 Forbidden
403 Forbidden
<---------------------
```

If a solution has to be provided to enable SPIT filtering then the following two sub-problems have to be solved:

- A authorization policy language that allows to expression the conditions and actions. An example is [I-D.ietf-simple-presence-rules].
- A mechanism to create, delete, update, retrieve and upload XML based authorization policy rules. XCAP [I-D.ietf-simple-xcap] is a possible solution.

In a more sophisticated setting one might even consider the following idea. Ideally, it would be good to stop unsolicited traffic as early as possible to avoid consuming bandwidth and processing power. Domains may agree to exchange authorization policies in order to stop SPIT earlier (i.e., closer to the source of the problem). The subsequent text describes this scenario.

```
A@example.com       Proxy          Proxy      B@otherdomain.com
@example.com  @otherdomain.com

| INVITE          |               |                |
| B@otherdomain.com               |                |
-------------------------->  INVITE
| B@otherdomain.com               |                |
-------------------------->  403 Forbidden
403 Forbidden
<---------------------
```

This call flow illustrates the bandwidth-saving interest of this use
Though, two scenarios could happen:

- In the good case, the sender’s domain is honest and exchanges authorization policies in order to apply rules that avoids forwarding unsolicited requests.

- In the worst case, the sender’s domain is not cooperative. It will refuse to upload such documents. In this case, the presence of rules in the recipient’s domain will suffice to keep the recipient "SPAM free", even if more traffic has been consumed (since the request has been relayed at least until the first proxy of the recipient’s domain, exactly like in the first use case).

These two use cases illustrate the advantages of using a standard mechanisms in this framework.

It might be desirable to use a hierarchy of authorization policy documents that need to be combined when applying them to the SIP signaling traffic. This raises the question of a merging algorithm, particularly when authorization policy rules are conflicting or contain blacklists.
4. Requirements

The design of anti-SPIT authorization policies is guided by the following requirements. Note that this is a first strawman proposal that requires further discussions (since some requirements are potentially controversial).

1. The policies SHOULD allow filtering incoming requests depending on several criteria’s:
   * Value of any SIP header attribute (e.g., From, To, Contact)
   * Method invoked by the caller (e.g., INVITE, MESSAGE)
   * Value of parameters specified in [I-D.schwartz-sipping-spit-saml]
     + IdentityStrength
     + CostOfCall
     + AuthenticationMethod
     + IdentityAssertion
     + ConnectionSecurity
     + SPITSuspected
     + CallCenter
     + AssertionStrength
   * Request URI of a request
   * Presence of a given expression in the body (subject for further investigation)

2. The policies SHOULD support wildcards (e.g., sip:*@example.com)

3. The policies SHOULD support logical operations (and, or, not) between individual elements in conditions

4. The policies SHOULD refer to all authenticated and unauthenticated identities.

5. The policies SHOULD allow the following actions to be specified:
* "block": stop forwarding the request and answer with a `403 Forbidden`
* "polite-block": drop the request without answering anything
* "mark": forward the request, putting a flag `SPAM`
* "allow": forward this message without conditions (this mechanism is described further)

* and trigger other mechanism, such as:

  + "puzzle": trigger the "Computational Puzzles" [I-D.jennings-sip-hashcash] mechanism.
  + "consent": trigger the "Consent Framework" [I-D.rosenberg-sipping-consent-framework] mechanism

6. The policies SHOULD allow a default action to be specified.

7. It SHOULD be possible to allow a hierarchy of authorization policies to be used.
5. Discussion and Open Issues

5.1. Extending Geopriv Authorization Policies

To fulfill requirements (1) to (6), it is necessary to decide if [I-D.ietf-geopriv-common-policy] and [I-D.ietf-simple-presence-rules] can be extended.

The following open issues have been identified:

- The authorization policies defined by the Geopriv working group focus on a whitelist approach. This document also raises the question of a backlisting capability that might need to be supported.

- The Geopriv Common Policy mechanism does not allow "deny" actions to be defined. This aspect refers to requirements (4) ("all") where (although "all except one" is supported by Common Policy).

- Requirement 2 (wildcards) is provided by Common Policy in a limited fashion by referring to the domain part of an identity. Regular expressions are not supported.

5.2. Hierarchical Authorization Policy Documents

If requirement (7) is valid then a conflict resolution mechanism needs to be evaluated. Geopriv Common Policy currently defines a very simple mechanism but it is for further investigation whether it is actually applicable to this problem domain. Other policy languages define a more sophisticated set of conflict resolution mechanisms with precedence and weights for policies. Although this might be an obviously solution for usage in the context of hierarchical authorization policies it causes problems in other places.
6. IANA Considerations

This document does not require actions by IANA.
7. Security Considerations

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.
8. Acknowledgements
9. References

9.1. Normative References


9.2. Informative References

[I-D.ietf-geopriv-common-policy]

[I-D.ietf-simple-presence-rules]

[I-D.ietf-simple-xcap]

[I-D.ietf-sip-identity]

[I-D.ietf-sipping-spam]

[I-D.jennings-sip-hashcash]

[I-D.rosenberg-sipping-consent-framework]

[I-D.schwartz-sipping-spit-saml]

Authors’ Addresses

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

Email: gdawirs@gdawirs.be

Thomas Froment
Alcatel
1, rue Ampere - BP 80056
Massy, Paris 91302
France

Email: Thomas.Froment@alcatel.fr

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

Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com
Intellectual Property Statement

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

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

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

Disclaimer of Validity

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

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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