SIPPING	H. Tschofenig	
Internet-Draft	Nokia Siemens Networks	
Intended status: Standards Track	D. Wing	
Expires: January 13, 2009	Cisco	
	H. Schulzrinne	
	Columbia University	
	T. Froment	
	Alcatel-Lucent	
	G. Dawirs	
	University of Namur	
	July 12, 2008	

TOC

A Document Format for Expressing Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony
draft-tschofenig-sipping-spit-policy-03.txt

Status of this Memo

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 defines an

authorization based policy language that allows end users to upload anti-SPIT policies to intermediaries, such as SIP proxies. These policies mitigate unwanted SIP communications. It extends the Common Policy authorization framework with additional conditions and actions. The new conditions match a particular Session Initiation Protocol (SIP) communication pattern based on a number of attributes. The range of attributes includes information provided, for example, by SIP itself, by the SIP identity mechanism, by information carried within SAML assertions.

Table of Contents

---

1. Introduction

TOC

The problem of SPAM for Internet Telephony (SPIT) is an imminent challenge and only the combination of several techniques can provide a framework for dealing with unwanted communication, as stated in [I-D.jennings-sip-hashcash] (Jennings, C., “Computational Puzzles for SPAM Reduction in SIP,” July 2007.).
One important building block is to have a mechanism that can instruct SIP intermediaries to react differently on incoming requests based on policies. Different entities, such as end users, parents on behalf of their children, system administrators in enterprise networks, etc., might create and modify authorization policies. The conditions in these policies can be created from many sources but some information elements are more important than others. For example, there is reason to believe that applying authorization policies based on the authenticated identity is an effective way to accept a communication attempt to deal with unsolicited communication. Authentication based on the SIP identity mechanism, see [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), is one important concept.
The requirements for the authorization policies described in this document are outlined in [I-D.froment-sipping-spit-requirements] (Tschofenig, H., Dawirs, G., Froment, T., Wing, D., and H. Schulzrinne, “Requirements for Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony,” July 2008.). A framework document is available at [I-D.tschofenig-sipping-framework-spit-reduction] (Tschofenig, H., Schulzrinne, H., Wing, D., Rosenberg, J., and D. Schwartz, “A Framework to tackle Spam and Unwanted Communication for Internet Telephony,” July 2008.).

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
This document reuses the terminology from RFC 4745 [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.):

> **Rule maker:**
> The RM is an entity that creates the authorization policies that react to unwanted connection attempts. The rule maker might be an end user that owns the 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). A standardized policy language is needed when the creation, modification and deletion of authorization policies are not only a local matter.
>
> **Authorization policy:**
> An authorization policy is given by a rule set. A rule set contains an unordered list of rules. Each rule has a condition, an action and a transformation component. The terms 'authorization policy', 'policy', 'rule set', 'authorization policy rule', 'policy rule' and 'rule' are used interchangeably. Authorization policies can be applied at the end host and/or by intermediaries.
>
> **Permission:**
> The term permission refers to the action and transformation components of a rule.

We use the term 'Recipient' for the entity that is target of the communication attempt of a sender.

---

3. Generic Processing

TOC

TOC

3.1. Structure of SPIT Authorization Documents

A SPIT authorization document is an XML document, formatted according to the schema defined in RFC 4745 [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.). SPIT authorization documents inherit the MIME type of common policy documents, application/auth-policy+xml. As described in [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.), this document is composed of rules which contain three parts - conditions, actions, and transformations. Each action or transformation, which is also called a permission, has the property of being a positive grant to the authorization server to perform the resulting actions, be it allow, block etc . As a result, there is a well-defined mechanism for combining actions and transformations obtained from several sources. This mechanism therefore can be used to filter connection attempts thus leading to effective SPIT prevention.

3.2. Rule Transport

TOC

Policies are XML documents that are stored at a Proxy Server or a dedicated device. The Rule Maker therefore needs to use a protocol to create, modify and delete the authorization policies defined in this document. Such a protocol is available with the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) [RFC4825] (Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," May 2007.).

---

4. Condition Elements

TOC

This section describes the additional enhancements of the conditions-part of the rule. This document inherits the Common Policy functionality, including <identity>, <validity>, and <sphere> conditions.
Note that, as discussed in [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.), a permission document applies to a translation if all the expressions in its conditions part evaluate to TRUE.

4.1. Identity

TOC

Although the <identity> element is defined in [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.), that specification indicates that the specific usages of the framework document need to define details that are protocol and usage specific. In particular, it is necessary for a usage of the common policy framework to:

- Define acceptable means of authentication.
- Define the procedure for representing the identity as a URI or IRI [RFC3987] (Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)," January 2005.).

This sub-section defines those details for systems based on [RFC3856] (Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)," August 2004.).

4.1.1. Acceptable Forms of Authentication

TOC

When used with SIP, a request is considered authenticated if one of the following techniques is used:

SIP Digest:
The proxy has authenticated the sender using SIP [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) digest authentication [RFC2617] (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.). However, if the anonymous authentication described on page 194 of RFC 3261 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) was used, the sender is not considered authenticated.

Asserted Identity:
If a request contains a P-Asserted-ID header field [RFC3325] (Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.) and

> the request is coming from a trusted element, the sender is considered authenticated.
>
> **Cryptographically Verified Identity:** If a request contains an Identity header field as defined in [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), and it validates the From header field of the request, the request is considered to be authenticated. Note that this is true even if the request contained a From header field of the form sip:anonymous@example.com. As long as the signature verifies that the request legitimately came from this identity, it is considered authenticated.

An anonymous From header field with RFC 4474 [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.) is considered authenticated, while anonymous digest is not considered authenticated, because the former still involves the usage of an actual username and credential as part of an authentication operation in the originating domain.

4.1.2. Computing a URI for the Sender

TOC

For messages that are authenticated using SIP Digest, the identity of the sender is set equal to the address of record (AoR) for the user that has authenticated themselves. The AoR is always a URI, and can be either a SIP URI or tel URI [RFC3966] (Schulzrinne, H., “The tel URI for Telephone Numbers,” December 2004.). For example, consider the following "user record" in a database:

```
SIP AOR: sip:alice@example.com
digest username: ali
digest password: f779ajvvh8a6s6
digest realm: example.com
```

If the proxy server receives an INVITE, challenges it with the realm set to "example.com", and the subsequent INVITE contains an Authorization header field with a username of "ali" and a digest response generated with the password "f779ajvvh8a6s6", the identity used in matching operations is "sip:alice@example.com".
For messages that are authenticated using RFC 3325 [RFC3325] (Jennings, C., Peterson, J., and M. Watson, “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks,” November 2002.), the identity of the sender is equal to the

URI in the P-Asserted-ID header field. If there are multiple values for the P-Asserted-ID header field (there can be one sip URI and one tel URI [RFC3966] (Schulzrinne, H., “The tel URI for Telephone Numbers,” December 2004.)), then each of them is used for the comparisons outlined in [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.), and if either of them match a <one> or <except> element, it is considered a match.

For messages that are authenticated using the SIP Identity mechanism [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), identity of the sender is equal to the SIP URI in the From header field of the request, assuming that the signature in the Identity header field has been validated.

In SIP systems, it is possible for a user to have aliases - that is, there are multiple SIP AoRs "assigned" to a single user. In terms of this specification, there is no relationship between those aliases. Each would look like a different user. This will be the consequence for systems where the sender is in a different domain than the recipient. However, even if the sender and recipient are in the same domain, and the proxy server knows that there are aliases for the sender, these aliases are not mapped to each other or used in any way.

SIP also allows for anonymous identities. If a message is anonymous because the digest challenge/response used the "anonymous" username, the message is considered unauthenticated and will match only an empty <identity> element. If a message is anonymous because it contains a Privacy header field [RFC3323] (Peterson, J., “A Privacy Mechanism for the Session Initiation Protocol (SIP),” November 2002.), but still contains a P-Asserted-ID header field, the identity in the P-Asserted-ID header field is still used in the authorization computations; the fact that the message was anonymous has no impact on the identity processing. However, if the message had traversed a trust boundary and the P-Asserted-ID header field and the Privacy header field had been removed, the message will be considered unauthenticated when it arrives at the proxy server. Finally, if a message contained an Identity header field that was validated, and the From header field contained a URI of the form sip:anonymous@example.com, then the sender is considered authenticated, and it will have an identity equal to sip:anonymous@example.com. Had such an identity been placed into a <one> or <except> element, there will be a match.

It is important to note that SIP frequently uses both SIP URI and tel URI [RFC3966] (Schulzrinne, H., “The tel URI for Telephone Numbers,” December 2004.) as identifiers, and to make matters more confusing, a SIP URI can contain a phone number in its user part, in the same format used in a tel URI. The sender's identity that is a SIP URI with a phone number will not match the <one> and <except> conditions whose 'id' is a tel URI with the same number. The same is true in the reverse. If the sender's identity is a tel URI, this will not match a SIP URI in the

<one> or <except> conditions whose user part is a phone number. URIs of different schemes are never equivalent.

4.2. Sphere

TOC

The <sphere> element is defined in [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.). However, each application making use of the common policy specification needs to determine how the policy server computes the value of the sphere to be used in the evaluation of the condition. To compute the value of <sphere>, the proxy server interacts with a presence server who knows whether at least one of the published presence documents includes the <sphere> element [RFC4480] (Schulzrinne, H., Gurbani, V., Kyzivat, P., and J. Rosenberg, "RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)," July 2006.) as part of the person data component [RFC4479] (Rosenberg, J., "A Data Model for Presence," July 2006.), and all of those containing the element have the same value for it, that is the value used for the sphere in policy policy processing. If, however, the <sphere> element was not available to the presence server (and hence not for the proxy server), or it was present but had inconsistent values, its value is considered undefined in terms of policy processing.

4.3. SPIT Handling

TOC

The <spit-handling> element is a way to react on the execution of certain SPIT handling mechanisms. For example, a rule might indicate that a CAPTCHA has to be sent to the sender and the sender subsequently has to return the result. Depending on the outcome of the robot test the rules might enforce different actions. This element provides such a condition capability.
The <spit-handling> condition evaluates to TRUE if any of its child elements evaluate to TRUE, i.e., the results of the individual child element are combined using a logical OR.
The <spit-handling> element MAY contain zero or more <challenge> elements. The <challenge> elements has an attribute 'result' that either contains "SUCCESS" or "FAILURE".

TOC

4.4. Presence Status

This condition evaluates to TRUE when the called user's current presence activity status is equal to the value in the <presence-status> element. Otherwise the condition evaluates to FALSE.

4.5. Time Period Condition

TOC

The <time-period> element allows to make decisions based on the time, date and timezone. It defines an extended version of the <validity> element.
The <time-period> element may contain the following attributes:

dtstart:
Start of interval (RFC 2445 [RFC2445] (Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)," November 1998.) DATE-TIME). This attribute is MANDATORY.

dtend:
End of interval (RFC 2445 [RFC2445] (Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)," November 1998.) DATE-TIME). This attribute is MANDATORY.

timestart:
Start of time interval in a particular day. It is of the TIME data type as mentioned in Section 4.3.12 of RFC 2445 [RFC2445] (Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)," November 1998.). This attribute is OPTIONAL. The default value is 000000.

timeend:
End of time interval in a particular day. It is of the TIME data type as mentioned in Section 4.3.12 of RFC 2445 [RFC2445] (Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)," November 1998.). This attribute is OPTIONAL. The default value is 235959.

byweekday: List of days of the week. This attribute is OPTIONAL.

The <time-period> is based on the description in CPL [RFC3880] (Lennox, J., Wu, X., and H. Schulzrinne, "Call Processing Language (CPL): A Language for User Control of Internet Telephony Services," October 2004.) but with a reduced feature set.
The "dtstart" and "dtend" attributes are formatted as iCalendar COS DATE-TIME values, as specified in Section 4.3.5 of RFC 2445 [RFC2445] (Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)," November 1998.). Only floating or UTC times can be used with time zones. The DATE-TIME is a subset of the corresponding syntaxes from ISO 8601 [ISO8601] (ISO (International Organization for Standardization), ""Data elements and interchange formats -- Information interchange -- Representation of dates and times", ISO Standard ISO 8601:2000(E), International Organization for Standardization, Geneva, Switzerland,," December 2000.).
The "timestart" specifes a time value to indicate the beginning of every day. The default value is 000000 representing the beginning of the day.
The "timeend" specifes a time value to indicate the end of every day. The default value is 235959 representing the end of the day.
The "byweekday" attribute specifies a comma-separated list of days of the week. "MO" indicates Monday, "TU" indicates Tuesday, "WE" indicates Wednesday, "TH" indicates Thursday, "FR" indicates Friday, "SA" indicates Saturday, and "SU" indicates Sunday. These values are not case-sensitive.
Here is an example of the time-period element.

```
<time dtstart="20070112T083000"
      timestart="0800"
      timeend="1800"
      byweekday="MO,TU,WE,TH,FR"
      dtend="20080101T183000"/>
```

The following aspects need to be considered:

1) By default, if all the OPTIONAL parameters are missing, <time-period> element is valid for the whole duration from 'dtstart' to 'dtend'.

2) The 'byweekday' attribute comes into effect only if the period from 'dtstart' till 'dtstart' is long enough to accommodate the specified values, else they are just neglected.

3) If the values of the 'byweekday' attribute values do not correspond to the expected domain, they are simply ignored.

4) Only a single 'byweekday' attribute MUST be listed in a <time> element.

5. Actions

TOC

As stated in [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), conditions are the 'if'-part of rules, whereas actions and transformations form their 'then'-part. The actions and transformations parts of a rule determine which operations the proxy server MUST execute on receiving a connection request attempt that matches all conditions of this rule. Actions and transformations permit certain operations to be executed.

5.1. Execute Action

TOC

The <handling> element allows a couple of actions to be triggered, namely

> **Block Action:**
> The block action states that this specific connection request MUST NOT be forwarded and a "403" forbidden message MUST be sent to the sender of the message.
>
> **Allow Action:**
> The Allow action states that this specific connection request MUST be forwarded.

Furthermore, a couple of further mechanisms, such as computational puzzles mechanism (described in [I-D.jennings-sip-hashcash] (Jennings, C., “Computational Puzzles for SPAM Reduction in SIP,” July 2007.)), the consent framework (described in [I-D.ietf-sip-consent-framework] (Rosenberg, J., Camarillo, G., and D. Willis, “A Framework for Consent-based Communications in the Session Initiation Protocol (SIP),” January 2008.)) etc. can be executed. Each mechanism needs to register a URI and the value of URI is placed in this field.
[Editior's Note: For editorial purposes the schema currently lists a few examples but in a non-URI format. When solution documents define these URIs then they can be used with this document.]

5.2. Forward To

TOC

The action supported in this section is forwarding of calls with the <forward-to> element that contains the following child element <target> that specifies the address of the forwarding rule. It should be a valid

SIP URI (RFC 3261 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.)) or TEL URI (RFC 3966 [RFC3966] (Schulzrinne, H., “The tel URI for Telephone Numbers,” December 2004.)).

---

6. Examples

TOC

This section provides a few examples for policy rules defined in this document.

6.1. Identity and Time-Based Policy

TOC

The following policy shows a white list with an identity condition and a simple time-based condition.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:spit="urn:ietf:params:xml:ns:spit-policy"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <rule id="AA56i09">
    <conditions>
      <identity>
          <one id="sip:bob@example.com"/>
          <many>
            <except domain="example.com"/>
            <except domain="example.org"/>
            <except id="sip:alice@bad.example.net"/>
            <except id="sip:bob@good.example.net"/>
            <except id="tel:+1-212-555-1234" />
            <except id="sip:alice@example.com"/>
          </many>
      </identity>
      <sphere value="work"/>
      <validity>
        <from>2003-12-24T17:00:00+01:00</from>
        <until>2003-12-24T19:00:00+01:00</until>
      </validity>
    </conditions>
    <actions>
      <spit:handling>allow</spit:handling>
    </actions>
    <transformations/>
  </rule>
</ruleset>
```

6.2. Extended Time-Based Policy

TOC

The following policy shows the usage of the <time-period> element to forward calls to an answering machine during the night.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:spit="urn:ietf:params:xml:ns:spit-policy"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <rule id="AA56i10">
    <conditions>
      <spit:time-period>
        <time dtstart="19970105T083000"
        timestart="2200"
        timeend="0800"
        byweekday="MO,TU,WE,TH,FR"
        dtend="19991230T183000"/>
       </spit:time-period>
    </conditions>
    <actions>
      <spit:forward-to>
        <target>sip:answering-machine@home.foo-bar.com
        </target>
      </spit:forward-to>
    </actions>
    <transformations/>
  </rule>
</ruleset>
```

6.3. Policy for triggering Captcha and Hashcash Challenges

TOC

The following example policy shows three rules with the rule id r1 - r4.

> Rule r1 matches for authenticated identities from the domain "example.com", "example.org" and the single identity "sip:bob@good.example.net". For these conditions SIP messages are forwarded to the SIP UA as indicated with the <handling> element.
>
> Rule r2 indicates that for SIP messages where the identity has not been verifiable the hash cash mechanism [I-D.jennings-sip-hashcash] (Jennings, C., “Computational Puzzles for SPAM Reduction in SIP,” July 2007.) and CAPTCHAs [I-D.tschofenig-sipping-captcha] (Tschofenig, H., Leppanen, E., Niccolini, S., and M. Arumaithurai, “Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) based Robot Challenges for SIP,” February 2008.) are applied (see the 'hashcash' and the 'captcha' token in the <execute> element).

> Rule r3 contains the <spit-handling> element with the <challenge> child element. This rule evaluates to TRUE if the sender returned a valid hash cash or a valid CAPTCHA result. The action part of the rule indicates that the call is then forwarded to the answering machine, namely sip:answering-machine@home.foo-bar.com.
>
> Rule r4 blocks the call if sender provided a wrong hash cash or CAPTCHA result.

Rule r1 and r2 are valid only from 2007-01-01T01:00:00+01:00 to 2007-07-01T24:00:00+01:00.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:spit="urn:ietf:params:xml:ns:spit-policy"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <rule id="r1">
    <conditions>
      <identity>
        <one id="sip:bob@good.example.net"/>
        <many domain="example.com"/>
        <many domain="example.org"/>
      </identity>
      <validity>
        <from>2007-01-01T01:00:00+01:00</from>
        <until>2007-07-01T24:00:00+01:00</until>
      </validity>
    </conditions>
    <actions>
      <spit:execute>allow</spit:execute>
    </actions>
    <transformations/>
  </rule>

  <rule id="r2">
    <conditions>
      <validity>
        <from>2007-01-01T01:00:00+01:00</from>
        <until>2007-07-01T24:00:00+01:00</until>
      </validity>
    </conditions>
    <actions>
      <spit:execute>hashcash</spit:execute>
      <spit:execute>captcha</spit:execute>
    </actions>
    <transformations/>
  </rule>

  <rule id="r3">
    <conditions>
      <spit:spit-handling>
        <challenge result="SUCCESS">hashcash</challenge>
        <challenge result="SUCCESS">captcha</challenge>
      </spit:spit-handling>
    </conditions>
    <actions>
      <spit:forward-to>
        <target>sip:answering-machine@home.foo-bar.com
        </target>
```

```
        </spit:forward-to>
      </actions>
      <transformations/>
    </rule>

    <rule id="r4">
      <conditions>
        <spit:spit-handling>
            <challenge result="FAILURE">hashcash</challenge>
            <challenge result="FAILURE">captcha</challenge>
        </spit:spit-handling>
      </conditions>
      <actions>
        <spit:execute>block</spit:execute>
      </actions>
      <transformations/>
    </rule>

  </ruleset>
```

---

7. XML Schema

TOC

This section contains the XML schema that defines the policies schema described in this document. This schema extends the Common Policy schema (see [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.)) by introducing new members of the <condition> and <action> elements.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:ietf:params:xml:ns:spit-policy"
  xmlns:spit="urn:ietf:params:xml:ns:spit-policy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <!-- This import brings in the XML language attribute xml:lang-->
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
    schemaLocation="http://www.w3.org/2001/xml.xsd"/>

  <xs:import namespace="urn:ietf:params:xml:ns:common-policy"/>

  <!-- Conditions -->

  <xs:element name="spit-handling">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="challenge" type="spit:challenge-type"
          minOccurs="0" maxOccurs="unbounded"/>
        <xs:any namespace="##other" processContents="lax"
          minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="result" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="SUCCESS"/>
            <xs:enumeration value="FAILURE"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="presence-status"
    type="spit:presence-status-activity-type"/>

  <xs:simpleType name="presence-status-activity-type">
    <xs:restriction base="xs:string"/>
  </xs:simpleType>

  <xs:simpleType name="challenge-type">
    <xs:restriction base="xs:string"/>
  </xs:simpleType>

  <xs:element name="time-period" type="spit:TimeSwitchType"/>

  <xs:complexType name="TimeType">
    <xs:annotation>
```

```
  <xs:documentation>Exactly one of the two attributes
    "dtend" and "duration" must occur. None of
    the attributes following freq are meaningful
    unless freq appears. </xs:documentation>
</xs:annotation>

<xs:attribute name="dtstart" type="xs:string" use="required">
  <xs:annotation>
    <xs:documentation>RFC 2445 DATE-TIME</xs:documentation>
  </xs:annotation>
</xs:attribute>

<xs:attribute name="dtend" type="xs:string" use="required">
  <xs:annotation>
    <xs:documentation>RFC 2445 DATE-TIME</xs:documentation>
  </xs:annotation>
</xs:attribute>

<xs:attribute name="timestart" type="xs:string" use="optional"
  default="000000">
  <xs:annotation>
    <xs:documentation>RFC 2445 TIME. It represents time in hours,
      minutes and seconds and denotes the beginning of the day
      time. The default value is 000000, denoting the
      beginning of the day. </xs:documentation>
  </xs:annotation>
</xs:attribute>

<xs:attribute name="timeend" type="xs:string" use="optional"
  default="235959">
  <xs:annotation>
    <xs:documentation>RFC 2445 TIME. It represents time in
      hours, minutes and seconds and denotes the
      end of the day time. The default value is 235959,
      denoting the end of the day. </xs:documentation>
  </xs:annotation>
</xs:attribute>


<xs:attribute name="byweekday" type="xs:string" use="optional">
  <xs:annotation>
    <xs:documentation>Comma-separated list of days of the week.
      Valid values are "MO", "TU",
      "WE", "TH", "FR", "SA" and "SU". These values are
      not case-sensitive. Each can be preceded
      by a positive (+n) or negative (-n) integer.
    </xs:documentation>
  </xs:annotation>
</xs:attribute>
```

```
    <xs:anyAttribute namespace="##any" processContents="lax"/>

  </xs:complexType>

  <xs:complexType name="TimeSwitchType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:sequence>
          <xs:element name="time" type="spit:TimeType"
            minOccurs="1" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <!-- Action -->

  <xs:element name="execute">
    <xs:simpleType>
      <xs:restriction base="xs:string">
      </xs:restriction>
    </xs:simpleType>
  </xs:element>

  <xs:element name="forward-to" type="spit:forward-to-type"/>

  <xs:complexType name="forward-to-type">
    <xs:sequence>
      <xs:element name="target" type="spit:target-type"/>
      <xs:any namespace="##other" processContents="lax"
        minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="target-type">
    <xs:restriction base="xs:anyURI"/>
  </xs:simpleType>

</xs:schema>
```

---

8. XCAP USAGE

TOC

The following section defines the details necessary for clients to manipulate SPIT authorization documents from a server using XCAP.

8.1. Application Unique ID

TOC

XCAP requires application usages to define a unique application usage ID (AUID) in either the IETF tree or a vendor tree. This specification defines the "Spit-policy" AUID within the IETF tree, via the IANA registration in Section 9 (IANA Considerations).

8.2. XML Schema

TOC

XCAP requires application usages to define a schema for their documents. The schema for Anti-SPIT authorization documents is described in Section 7 (XML Schema).

8.3. Default Namespace

TOC

XCAP requires application usages to define the default namespace for their documents. The default namespace is urn:ietf:params:xml:ns:spit-policy.

8.4. MIME Type

TOC

XCAP requires application usages to defined the MIME type for documents they carry. Anti-SPIT privacy authorization documents inherit the MIME type of Common Policy documents, application/auth-policy+xml.

8.5. Validation Constraints

TOC

This specification does not define additional constraints.

8.6. Data Semantics

TOC

This document discusses the semantics of Anti-SPIT authorization.

8.7. Naming Conventions

TOC

When a SIP Proxy receives a SIP message to route it towards to a specific user foo, it will look for all documents within http://[xcaproot]/spit-policy/users/foo, and use all documents found beneath that point to guide authorization policy.

8.8. Resource Interdependencies

TOC

This application usage does not define additional resource interdependencies.

8.9. Authorization Policies

TOC

This application usage does not modify the default XCAP authorization policy, which is that only a user can read, write or modify his/her own documents. A server can allow privileged users to modify documents that they do not own, but the establishment and indication of such policies is outside the scope of this document.

---

9. IANA Considerations

TOC

There are several IANA considerations associated with this specification.

9.1. Anti-SPIT Policy XML Schema Registration

TOC

URI: urn:ietf:params:xml:schema:spit-policy

Registrant Contact: Hannes Tschofenig (hannes.tschofenig@nsn.com).

XML: The XML schema to be registered is contained in Section 7 (XML Schema). Its first line is

```
<?xml version="1.0" encoding="UTF-8"?>
```

and its last line is

```
        </xs:schema>
```

9.2. Anti-SPIT Policy Namespace Registration

TOC

URI: urn:ietf:params:xml:ns:spit-policy

Registrant Contact: Hannes Tschofenig (hannes.tschofenig@nsn.com).

XML:

9.3. XCAP Application Usage ID

TOC

This section registers an XCAP Application Usage ID (AUID) according to the IANA procedures defined in [RFC4825] (Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," May 2007.).
Name of the AUID: spit-policy
Description: The rules defined in this documents describe ways to react on unwanted and unsolicted communication (including Spam).

---

10. Security Considerations

TOC

This document aims to make it simple for users to influence the behavior of SIP message routing with an emphasis on SPIT prevention. This document proposes a strawman proposal for conditions and actions that might be useful when it comes to allowing a UA to tell its proxies which messages it wants to receive and what tasks it wants those proxies to perform before sending a SIP request to the UA.
A couple of requirements are described in [I-D.froment-sipping-spit-requirements] (Tschofenig, H., Dawirs, G., Froment, T., Wing, D., and H. Schulzrinne, "Requirements for Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony," July 2008.) and a general discussion about the available solution mechanisms is available with [RFC5039] (Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam," January 2008.). This document offers the ability to glue the different solution pieces together.

Since this document uses the Common Policy framework it also inherits its capabilities, including the combining permission algorithm that is applied when multiple rules fire. Unauthorized access to the user's Anti-SPIT rules must be prevented to avoid the introduction of security vulnerabilities.

---

11. Contributors

TOC

We would like to thank Mayutan Arumaithurai (mayutan.arumaithurai@gmail.com) for his work on this document.

---

12. Acknowledgments

TOC

We would like to thank

- Jonathan Rosenberg, David Schwartz and Dan York for sharing their thoughts with us before the first version of this document was written.
- Miguel Garcia and Rémi Denis-Courmont for their review comments to the -00 version.
- Mayutan Arumaithurai for his editing help with the -00 version.
- Poikselka Miikka, Isomaki Markus, Jari Mutikainen, Jean-Marie Stupka, and Antti Laurila for their comments and for pointing us to specifications outside the IETF.

This document intentionally re-uses concept from existing documents. In particular, we reused

- ideas from SIEVE [RFC5228] (Guenther, P. and T. Showalter, “Sieve: An Email Filtering Language,” January 2008.), a mail filtering language.
- the text in Section 4.5 (Time Period Condition) is based on the description in the Call Processing Language (CPL) [RFC3880] (Lennox, J., Wu, X., and H. Schulzrinne, “Call Processing Language (CPL): A Language for User Control of Internet Telephony Services,” October 2004.). In general, the difference between CPL and this document is that CPL has a more procedural approach, while this proposal is matching-based. It is obviously possible to enhance CPL as well to provide the functionality offered in this document.

*text in Section 4.1 (Identity) from [RFC5025] (Rosenberg, J., "Presence Authorization Rules," December 2007.).

*content of Section 5.2 (Forward To), and Section 4.4 (Presence Status) is reused from [ETSI-TS-183-004] (ETSI, "TS 183 004, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification," 2007.).

---

13. References

TOC

13.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.
[RFC2617]	Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," RFC 2617, June 1999 (TXT, HTML, XML).
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2002 (TXT).
[RFC3323]	Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)," RFC 3323, November 2002 (TXT).
[RFC3856]	Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)," RFC 3856, August 2004 (TXT).
[RFC3966]	Schulzrinne, H., "The tel URI for Telephone Numbers," RFC 3966, December 2004 (TXT).
[RFC3987]	Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)," RFC 3987, January 2005 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," RFC 4474, August 2006 (TXT).
[RFC4479]	Rosenberg, J., "A Data Model for Presence," RFC 4479, July 2006 (TXT).
[RFC4480]	Schulzrinne, H., Gurbani, V., Kyzivat, P., and J. Rosenberg, "RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)," RFC 4480, July 2006 (TXT).
[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 (TXT).
[RFC4825]	Rosenberg, J., “The Extensible Markup Language (XML) Configuration Access Protocol (XCAP),” RFC 4825, May 2007 (TXT).

13.2. Informative References

TOC

[ETSI-TS-183-004]	ETSI, "TS 183 004, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification," 2007.
[I-D.froment-sipping-spit-requirements]	Tschofenig, H., Dawirs, G., Froment, T., Wing, D., and H. Schulzrinne, "Requirements for Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony," draft-froment-sipping-spit-requirements-03 (work in progress), July 2008 (TXT).
[I-D.ietf-sip-consent-framework]	Rosenberg, J., Camarillo, G., and D. Willis, "A Framework for Consent-based Communications in the Session Initiation Protocol (SIP)," draft-ietf-sip-consent-framework-04 (work in progress), January 2008 (TXT).
[I-D.jennings-sip-hashcash]	Jennings, C., "Computational Puzzles for SPAM Reduction in SIP," draft-jennings-sip-hashcash-06 (work in progress), July 2007 (TXT).
[I-D.tschofenig-sipping-captcha]	Tschofenig, H., Leppanen, E., Niccolini, S., and M. Arumaithurai, "Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) based Robot Challenges for SIP," draft-tschofenig-sipping-captcha-01 (work in progress), February 2008 (TXT).
[I-D.tschofenig-sipping-framework-spit-reduction]	Tschofenig, H., Schulzrinne, H., Wing, D., Rosenberg, J., and D. Schwartz, "A Framework to tackle Spam and Unwanted Communication for Internet Telephony," draft-tschofenig-sipping-framework-spit-reduction-04 (work in progress), July 2008 (TXT).
[ISO8601]	ISO (International Organization for Standardization), "Data elements and interchange formats -- Information interchange -- Representation of dates and times", ISO Standard ISO 8601:2000(E), International Organization for Standardization, Geneva, Switzerland,," December 2000.
[OMA-TS-XDM_Shared_Policy]	Open Mobile Alliance, "Shared Policy XDM Specification," 2007.
[RFC2445]	Dawson, F. and Stenerson, D., "Internet Calendaring and Scheduling Core Object

	Specification (iCalendar)," RFC 2445, November 1998 (TXT, HTML, XML).
[RFC3325]	Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," RFC 3325, November 2002 (TXT).
[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 (TXT).
[RFC5025]	Rosenberg, J., "Presence Authorization Rules," RFC 5025, December 2007 (TXT).
[RFC5039]	Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam," RFC 5039, January 2008 (TXT).
[RFC5228]	Guenther, P. and T. Showalter, "Sieve: An Email Filtering Language," RFC 5228, January 2008 (TXT).

Authors' Addresses

TOC

	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at
	Dan Wing
	Cisco
Phone:	
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

	Thomas Froment
	Alcatel-Lucent
	1, rue Ampere - BP 80056
	Massy, Paris 91302
	France
Email:	Thomas.Froment@alcatel-lucent.fr
	Geoffrey Dawirs
	University of Namur
	21, rue Grandgagnage
	Namur B-5000
	Belgique
Email:	gdawirs@gdawirs.be

Full Copyright Statement

TOC

Intellectual Property

that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.