

SIPPING Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 17, 2008

S. Niccolini
NEC
K. Fischer
Siemens Enterprise Communications
D. Wing
Cisco System, Inc.
M. Stiernerling
NEC
H. Tschofenig
Nokia Siemens Networks
February 14, 2008

Spam feedback for SIP
draft-niccolini-sipping-spam-feedback-00

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/lid-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 17, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document gives an overview of possible mechanisms for SIP UAs to

Internet-Draft

Spam feedback for SIP

February 2008

feedback spam information to the system (e.g. other SIP entities like upstream SIP proxies) thus they can use this information for handling subsequent calls (e.g. blacklist the caller, input this info to reputation systems, compute spam-specific caller statistics, etc.).

Table of Contents

1.	Introduction	3
2.	SIP Spam Feedback: sending operations	3
2.1.	Alternatives for sending spam feedbacks	4
2.1.1.	ABNF	4
2.1.2.	Event package usage	4
2.1.2.1.	Overview	4
2.1.2.2.	Subscribe behavior	5
2.1.2.3.	Notify behavior	6
3.	SIP Spam Feedback: system operations	6
4.	Advantages and disadvantages of alternatives	7
5.	Additional considerations of feedback operations	8
6.	Security Considerations	8
7.	IANA Considerations	9
8.	References	9
8.1.	Normative References	9
8.2.	Informative References	9
	Authors' Addresses	9
	Intellectual Property and Copyright Statements	12

1. Introduction

For the purpose of SPIT prevention it would be nice to have a mechanism for users to report the fact that they received a spam call. For example, a button on the user interface of the client (either hardware or software) might empower callees to inform the system that a particular caller initiated a spam call to the callee (see also [[RFC5039](#)]). This information can be used in many ways depending on the configuration of the system and on user preferences (e.g. can be used to add the caller to the callee's personal black list, to inform a reputation system, to apply particular call handling to subsequent calls of such caller either making him solving a CAPTCHA before initiating new calls or making him solving a computational puzzle, etc.). The discussion on how to use the user feedback depending on the configuration of the system and on user preferences is out of the scope of this document. The scope of this document is to highlight possible alternatives how this feedback should be delivered to the system in order to make a decision how this feedback should be implemented.

2. SIP Spam Feedback: sending operations

A UA generates a spam feedback after the user press the "spam" button. The spam feedback SHOULD carry information about the call and its originator. Information that are redundant SHOULD be avoided. Such information are taken into account by the system in order to apply different policies depending on system configuration or on user preferences. Examples of information about the call are, but not limited to, listed here:

- o caller SIP URI;
- o callee SIP URI;
- o Call-ID;
- o call start time (exact definition of call start time has to be included);
- o call end time (exact definition of call start time has to be


```

        Caller-sign-val / Callee-sign-val /
        Caller-media-val / Callee-media-val /
        Via / Route / Record-Route /
        Alert-Info / ...
Call-start-val    = "Call-start" EQUAL date
Call-end-val      = "Call-end" EQUAL date
Caller-sign-val   = "Caller-sign" EQUAL hostport
Callee-sign-val  = "Callee-sign" EQUAL hostport
Caller-media-val  = "Caller-media" EQUAL hostport
Callee-media-val = "Callee-media" EQUAL hostport

```

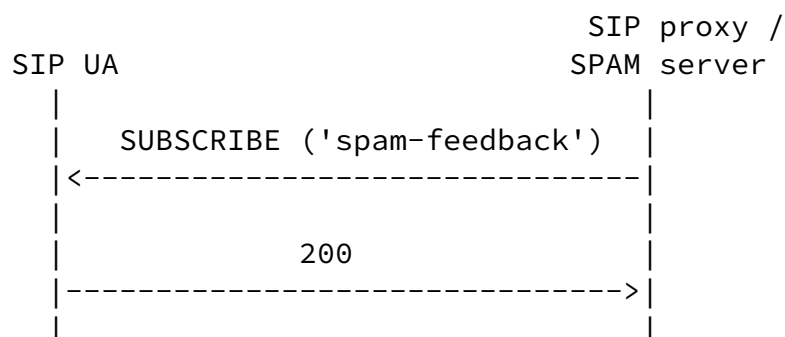
Figure 1: ABNF

[2.1.2.](#) Event package usage

[2.1.2.1.](#) Overview

[RFC3265] specifies an extension to SIP providing an extensible framework by which SIP nodes can request notification from remote

nodes indicating that certain events have been occurred. This framework can be applied to realize an notification mechanism of spam feedback from a SIP UA towards a server like a SIP proxy. A server interested in feedback if a call is considered as spit / spam by the user, subscribes to the new defined event package 'spam-feedback' at the SIP UA. After the user has pressed the "spam" button, the SIP UA notifies the server about the spam call. The NOTIFY message includes also some information to correlate the feedback with a specific call and to provide additional information. Figure 2 depicts the general call flow, which is explained in the following sections. Call signaling specific messages like INVITE, 18x or 200 responses are omitted from the figure for simplicity.



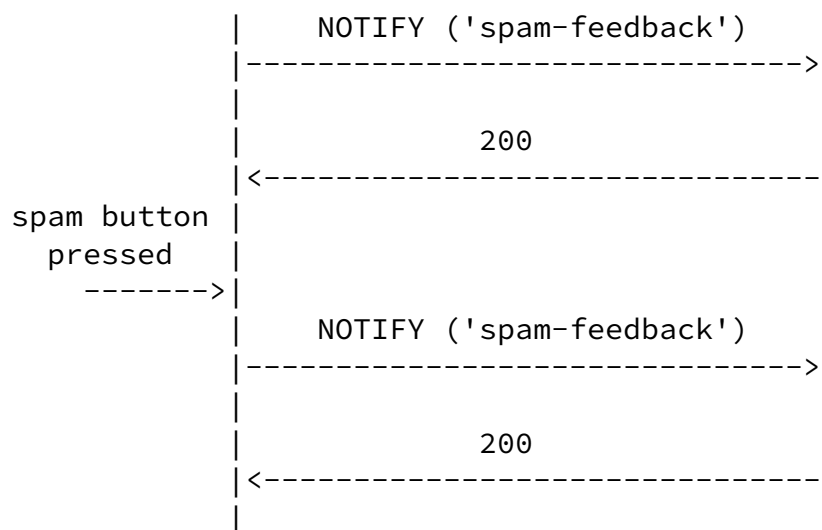


Figure 2: Overview call flow spam feedback event mechanism

[2.1.2.2.](#) Subscribe behavior

A SPAM / SIP server interested in spam feedback from a SIP UA sends a SUBSCRIBE request to the dedicated SIP UA. The request contains a Event header indicating that the 'spam-feedback' event package shall be subscribed. The request may contain also an Expires header indicating the duration of the subscription. If no Expires header is present, the subscription has an unlimited duration. At any time before a subscription expires, the subscriber may refresh the timer

on such a subscription by sending another SUBSCRIBE request on the same dialog as the existing subscription.

On receipt of a SUBSCRIBE request the SIP UA should check that the event package specified in the Event header is understood. If not, a "489 Bad Event" response should be returned. The SIP UA should check if the requesting server is authorized to subscribe to the event package. Prior to authorization the SIP UA needs to authenticate the server. One way achieving this is to use a TLS connection to the spam / SIP server, which might be already established to protect SIP registration and call signaling. Usually, the server is authenticated during TLS handshake, e.g. by a X.509 certificate, whereas the SIP UA is authenticated by SIP digest ([[RFC3261](#)] and [[RFC2617](#)]) on top of TLS. TLS provides also additional security properties, which addresses the security considerations of [[RFC3265](#)]

(please refer to [Section 6](#)).

Based on the configured policy the SIP UA accepts the SUBSCRIBE request by sending a 200 response, temporarily accepts the request with a 202 response or declines it by sending a non 200 class response like "403 Forbidden" or "603 Declined".

[2.1.2.3](#). Notify behavior

After the SIP UA has accepted the subscription, a NOTIFY message is sent directly after the 200 response to indicate the initial state. The NOTIFY Event header contains the 'spam-feedback' package name. The body should be empty, because no spam feedback needs to be notified initially. The NOTIFY message is sent over the already established TLS connection.

When a user receives a call considered as spam, he presses the "spam" button, which initiates a new NOTIFY message from the UA to the server. In contrast to the initial NOTIFY message, the body contains information about the call and its originator. Such information are taken into account by the spam system in order to apply different policies depending on system configuration or on user preferences. Refer to [Section 2](#) for a list of carried information.

[[Note: The concrete specification of the 'spam-feedback' event package will be added in a future version.]]

[3](#). SIP Spam Feedback: system operations

The system (e.g. a SIP proxy) that receives a notification of a certain call being spam should apply the policies defined in the system configuration and in the user preferences in order to handle

subsequent calls coming from that caller. Examples of behavior include:

- o insert the caller in the callee's personal blacklist;
- o input the feedback to a reputation system computing the reputation of the callers;
- o configure the system to apply particular actions on subsequent calls initiated by such a caller (e.g. route to voicemail, challenge with a CAPTCHA, challenge with a computational puzzle,

etc.)

4. Advantages and disadvantages of alternatives

We provide here a list of advantages and disadvantages in order to stimulate discussion on which technique should be used to send feedback.

Advantages for using BYE are:

- o the mechanism can piggyback on a message that is already present and that the UA is sending anyway;
- o it gives users a positive feeling/knowledge (if realized using a special button) that there is a special entity in the network that takes care of spam information (other than the proxy only) and (theoretically) will do something useful with it.

Disadvantages for using BYE are:

- o the mechanisms has to be piggybacked on the BYE; this means the user has to decide if the call is spam at the same time the user terminates the call. This could be difficult with some user interfaces;
- o the feedback information can in principle be routed upstream to a SIP proxy that can make use of it (if the sender proxy is the one controlled by the spammer this would mean giving him information on how the call was evaluated). Thus it is necessary to strip feedback information when the BYE leaves the caller's administrative domain (this puts additional load on the proxy). Failure to strip that information will allow the caller to realize if their call was marked as spam by the called party (privacy and security risk).

Advantages for using NOTIFY are:

- o feedback information is sent only to SIP proxy or other special devices that are the intended recipients of such a message and that can make use of it;
- o it can be delivered after the BYE (e.g. using a special dialing sequence;

- o there is no need to require header stripping at the network

- administrative boundary;
- o it is easier (with respect to the usage of BYE) to authorize the mechanisms;
- o it gives users a positive feeling/knowledge that there is a special entity in the network that takes care of spam information (other than the proxy only) and (theoretically) will do something useful with it

Disadvantages for using NOTIFY are:

- o it requires an additional message;
- o it requires additional infrastructural devices to be deployed (even if their introduction would not be too difficult since they are orthogonal to the signalling path).

From a first analysis the usage of NOTIFY seems to be preferred but it is up to discussion in the community to reach consensus on this topic.

5. Additional considerations of feedback operations

This document does not address important considerations on how and if the system (e.g. the SIP proxy serving the UA that received the spam call) should pass the information of a certain call being spam to other upstream proxies (e.g. to the SIP proxy in the originating domain). Such considerations are out of the scope of this document. The authors envision that such discussion should take place in another draft and investigate if additional headers or error messages should be defined to report upstream proxies about a call being considered spam by a certain domain or not. Also passing spam scoring information to upstream proxies is a possibility that should be considered in such draft and the appropriate security considerations should be applied.

6. Security Considerations

Some session requests may be spam for some users but not for others, it should be clear that the feedback is not providing a general security assessment of the call being spam or of the caller being abusive, but a personal one. The system should process spam feedbacks preserving normal operations for all users without letting some "mafia" users exploiting this mechanism to create DoS attacks denying users to call. The feedback message should be therefore challenged and authentication mechanisms should be applied. Also if the spam feedback is used to blacklist caller or entire domains, it should be used very carefully.

The security considerations described in [\[RFC3265\]](#) are inherited and need also be considered by applying the general notification framework for spam feedback. Most of the security threats are directly addressed by an authenticated TLS connection between the notifier and the subscriber.

[[Note: Additional text regarding each threat of [RFC 3265](#) is added in a later version]]

[7.](#) IANA Considerations

[[This section will be completed in a later version of this document.]]

[8.](#) References

[8.1.](#) Normative References

- [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.
- [RFC3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", [RFC 3265](#), June 2002.

[8.2.](#) Informative References

- [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.
- [RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", [RFC 5039](#), January 2008.

Internet-Draft

Spam feedback for SIP

February 2008

Authors' Addresses

Saverio Niccolini
NEC Laboratories Europe, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 4342 118
Email: saverio.niccolini@nw.neclab.eu
URI: <http://www.nw.neclab.eu>

Kai Fischer
Siemens Enterprise Communications GmbH & Co. KG
Schertlinstr. 8
Munich 81379
Germany

Phone: +49 (0) 89 722-37360
Email: kai.fischer@siemens.com

Dan Wing
Cisco System, Inc.
170 West Tasman Drive
San Jose, CA 95134
US

Email: dwing@cisco.com

Martin Stiernerling
NEC Laboratories Europe, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 4342 113

Email: stiemerling@nw.neclab.eu
URI: <http://www.nw.neclab.eu>

Niccolini, et al.

Expires August 17, 2008

[Page 10]

Internet-Draft

Spam feedback for SIP

February 2008

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

Email: Hannes.Tschofenig@nsn.com

Internet-Draft

Spam feedback for SIP

February 2008

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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.

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, THE IETF TRUST 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.

Intellectual Property

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.

Acknowledgment

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