

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: February 19, 2008

D. Wing  
Cisco Systems  
S. Niccolini  
NEC  
H. Tschofenig  
Nokia Siemens Networks  
M. Stiernerling  
NEC  
August 18, 2007

Spam Score for SIP  
draft-wing-sipping-spam-score-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/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 February 19, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document defines a mechanism for SIP proxies to communicate a spam score to downstream SIP proxies and SIP user agents so they can provide alternate call routing or call handling.

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](#)].

Table of Contents

[1.](#) Introduction . . . . . [3](#)

[2.](#) Operation of Spam-Scoring Proxy . . . . . [3](#)

[3.](#) Operation of Proxy or User Agent . . . . . [3](#)

[4.](#) ABNF . . . . . [4](#)

[5.](#) Examples . . . . . [5](#)

[6.](#) Security Considerations . . . . . [5](#)

[7.](#) Acknowledgements . . . . . [5](#)

[8.](#) IANA Considerations . . . . . [5](#)

[9.](#) References . . . . . [6](#)

[9.1.](#) Normative References . . . . . [6](#)

[9.2.](#) Informational References . . . . . [6](#)

Authors' Addresses . . . . . [6](#)

Intellectual Property and Copyright Statements . . . . . [8](#)

Internet-Draft

SIP Spam Score

August 2007

## 1. Introduction

It is desirable for SIP proxies to insert a spam score so that downstream SIP proxies and downstream SIP user agents can use a high score to decide that special handling is required. For example, a score above 20 might cause one of the spam avoidance techniques, described in [[I-D.ietf-sipping-spam](#)], to be triggered for this call.

This specification allows each SIP proxy to contribute spam scoring information that can be useful to downstream SIP proxies and the SIP UA. The downstream SIP proxies might ignore that information (e.g., they don't trust it) or might use it (e.g., they trust it because it was generated by a federation).

From a deployment point of view it is expected that the score will most likely be beneficial (and trustworthy) when inserted by a SIP proxy on the recipients side for evaluation by a SIP UA that has a direct relationship with this SIP proxy.

## 2. Operation of Spam-Scoring Proxy

A SIP proxy generates a spam score using a local mechanism. Negative scores indicate the SIP request is not considered spam, and positive scores indicate the SIP request is considered spam. The higher the value, the more likely a message is spam or is not spam.

This spam score is inserted into the "Via:" header, which is already generated by the proxy.

The Via header was chosen because it the Via is already correlated with the proxy that generated the Via header.

## 3. Operation of Proxy or User Agent

A downstream proxy MAY use the spam score or spam-detail information to change call routing or call handling. It is RECOMMENDED that only scores generated by trusted proxies be used. The behavior of the SIP proxy or user agent when the spam score is above a certain value is a local matter. Examples of behavior include:

- o a SIP request with a high spam score might cause a proxy or user agent to redirect the SIP request to company's main telephone extension or to the user's voicemail
- o a user agent might alert the user by flashing the phone (without audible ringing)

- o a user agent might allow calls with a spam score below a certain value during daylight hours, but deny such calls at night.
- o a proxy might challenge the caller to complete a Turing test.

These aspects are discussed in  
[\[I-D.tschofenig-sipping-framework-spit-reduction\]](#).

#### [4.](#) ABNF

ABNF using the ABNF syntax of [\[RFC3261\]](#):

via-extension	= spam-score / spam-detail
spam-score	= "spam" EQUAL score
score	= *"- " 1*4DIGIT [ "." 0*3DIGIT ]
spam-detail	= "spam-detail" EQUAL detail
detail	= QUOTE mech SEMI rule-score *(COMMA rule-score) QUOTE
rule-score	= rule [ "=" score ]
mech	= token
rule	= token

Figure 1: ABNF

## [5.](#) Examples

The following example shows a SIP score generated by biloxi.com and atlanta.com. In this example, atlanta.com is owned by a spammer who is trying to fool downstream systems with their low spam score (0.0). However, the biloxi.com proxies and user agents only pay attention to spam scores from Via: headers generated by biloxi.com proxies, so atlanta.com's attempts are in vain.

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP biloxi.com;branch=z9hG4bKnashds8
    ;received=192.0.2.1
    ;spam=-5
    ;spam-detail="Hormel-1.0;whitelist=-10,call_volume=5"
Via: SIP/2.0/UDP sip.atlanta.com;branch=z9hG4bKfjzc
    ;received=192.0.3.2
    ;spam=-100
    ;spam-detail="Jaeger-3.3;not-a-spammer=-100"
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
```

CSeq: 314159 INVITE  
Contact: <sip:alice@pc33.atlanta.com>  
Content-Type: application/sdp  
Content-Length: 142

Figure 2: example

## 6. Security Considerations

SIP proxies and SIP user agents need to ignore spam scores in Via headers generated by proxies that aren't trusted. Via headers have the most recent proxy on top, so parsing for spam scores should stop at the first Via header from a non-trusted proxy.

## 7. Acknowledgements

Add your name here.

## 8. IANA Considerations

This document will add new IANA registrations for new SIP headers.

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

document.]]

## 9. References

### 9.1. Normative References

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

[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.

## [9.2.](#) Informational References

- [I-D.ietf-sipping-spam]  
Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", [draft-ietf-sipping-spam-05](#) (work in progress), July 2007.
- [I-D.tschofenig-sipping-framework-spit-reduction]  
Tschofenig, H., "A Framework to tackle Spam and Unwanted Communication for Internet Telephony", [draft-tschofenig-sipping-framework-spit-reduction-01](#) (work in progress), July 2007.

### Authors' Addresses

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

Email: [dwing@cisco.com](mailto:dwing@cisco.com)

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

Phone: +49 (0) 6221 4342 118

Email: [saverio.niccolini@netlab.nec.de](mailto:saverio.niccolini@netlab.nec.de)

URI: <http://www.netlab.nec.de>

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

Email: [Hannes.Tschofenig@nsn.com](mailto:Hannes.Tschofenig@nsn.com)

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

Phone: +49 (0) 6221 4342 113  
Email: [stiernerling@netlab.nec.de](mailto:stiernerling@netlab.nec.de)  
URI: <http://www.netlab.nec.de>



Copyright (C) The IETF Trust (2007).

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](mailto:ietf-ipr@ietf.org).

## Acknowledgment

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