RUCUS Exploratory Working Group
Internet-Draft
Intended status: Experimental
Expires: August 16, 2008

D. Wing
Cisco
S. Niccolini
M. Stiemerling
NEC
H. Tschofenig
Nokia Siemens Networks
February 13, 2008

Spam Score for SIP
draft-wing-sipping-spam-score-01

Status of this Memo

Copyright Notice

Abstract

This document defines a mechanism for SIP proxies to communicate a spam score to downstream SIP proxies and to SIP user agents. This information can then be used as input to other decision making engines, for example, to provide alternate call routing or call

handling.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Operation of Spam-Scoring Proxy 3
4. Operation of Proxy or User Agent 4
5. Grammar 5
6. Examples 5
7. Security Considerations 6
8. Acknowledgements 6
9. IANA Considerations 6
10. References 6
10.1. Normative References 6
10.2. Informational References 7
Appendix A. Changes 7
A.1. Changes from -00 to -01 7
Authors' Addresses 7
Intellectual Property and Copyright Statements 9

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 [RFC5039] 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 user agent (UA). The downstream SIP proxies or SIP UA might ignore that information (e.g., it doesn't trust the SIP proxy that generated the spam score) or might use it.

Note that this document does not make the attempt to define how the spam score was derived nor to distribute information that could be used to verify the spam score generation. Furthermore, this document does not attempt to cryptographically bind the identity of the entity generating the score to the value itself. Hence, its usage is likely to be useful only between neighboring administrative domains communicating such a score.

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 [RFC2119].

3. Operation of Spam-Scoring Proxy

A SIP proxy evaluates an incoming SIP request and generates a spam score using a local mechanism. This score is between 0 (indicating the message is not spam) and 100 (indicating the message is spam). Values between 0 and 100 indicate the 'likelihood' that the SIP

request is spam, with higher values indicating a higher likelihood the message is spam.

This spam score is inserted into the new "Spam-Score" header. This header field contains a summary spam score and optionally contains detail information. The detail information is implementation dependent. The detail information is valuable for debugging and to provide the SIP user agent or SIP proxy with additional information regarding how the spam-scoring SIP proxy's local mechanism arrived at the summary spam score.

4. Operation of Proxy or User Agent

A downstream proxy or the SIP user agent MAY use the spam score or spam-detail information to change call routing or call handling. It is envisioned that some form of policies indicate the trusted proxies in order to decide which spam scores to consider for special call treatment.

> In some jurisdictions, the end user needs to authorize call handling, including rejection of a call based on a spam score. Mechanisms to allow users to influence such policies are, however, out of scope of this document.

The behavior of the SIP proxy or user agent when the spam score is above a certain value is a local policy matter. Examples of behavior include:

- 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
- a user agent might alert the user by flashing the phone (without audible ringing)
- a user agent might allow calls with a spam score below a certain value during daylight hours, but deny such calls at night.
- a proxy might challenge the caller to complete a Turing test.

5. Grammar

ABNF using the ABNF syntax of [RFC3261]:

```
extension-header   = spam-score [ SP ";" spam-detail ]

spam-score         = score SP "by" SP hostname
score              = 1*3DIGIT [ "." 0*3DIGIT ]

spam-detail        = "detail" EQUAL detail
detail             = QUOTE mech SEMI rule-score
                     *(COMMA rule-score) QUOTE
                     ; mathematical average of the rule-scores
                     ; MUST be same as spam-score

rule-score         = rule [ "=" score ]
mech               = token
rule               = token
```

Figure 1: ABNF

6. Examples

The following example shows a SIP score generated and inserted by two SIP proxies, sip.example.com and sip.example.net. In this example, sip.example.com is owned by a spammer who is trying to fool downstream systems with their low spam score (0). However, the example.net proxies and user agents only pay attention to spam scores from Spam-Score headers generated by example.net proxies, so example.com's attempts to fool the downstream proxies (with its low spam score) are in vain.


```
INVITE sip:bob@example.net SIP/2.0
Via: SIP/2.0/UDP sip.example.net;branch=z9hG4bKnashds8
  ;received=192.0.2.1
Spam-Score: 75 by sip.example.net
  ;detail="SIPfilter-1.0;call_volume=75"
Via: SIP/2.0/UDP sip.example.com;branch=z9hG4bKfjzc
  ;received=192.0.2.127
Max-Forwards: 70
To: Bob <sip:bob@example.net>
From: Alice <sip:alice@example.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.example.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.example.com>
Content-Type: application/sdp
Content-Length: 142
```

```
[... SDP elided from this example...]
```

Figure 2: Example with spam scores

7. Security Considerations

SIP proxies and SIP user agents need to ignore spam scores generated by proxies that aren't trusted.

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

8. Acknowledgements

Thanks to Joachim Charzinski, Daniel Quinlan, and S. Moonesamy for their suggestions to improve this document.

9. IANA Considerations

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

10. References

10.1. 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.

10.2. Informational References

[RFC5039] Rosenberg, J. and C. Jennings, "The Session Initiation

Protocol (SIP) and Spam", RFC 5039, January 2008.

Appendix A. Changes

Note to RFC Editor: please remove this section prior to publication.

A.1. Changes from -00 to -01

- Changed scoring from positive/negative to 0-100 range.
- Moved score from a "Via:" extension to a new header "Spam-Score:".
- Changed from Standards Track to Experimental.

Authors' Addresses

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

Email: 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
URI: http://www.netlab.nec.de

Martin Stiemerling

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

Phone: +49 (0) 6221 4342 113
Email: stiemerling@netlab.nec.de
URI: http://www.netlab.nec.de

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.com

Full Copyright Statement

Intellectual Property

Acknowledgments

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

using xml2rfc v1.33pre66 (of http://xml.resource.org/) from a source in RFC-2629 XML format.