REPUTE Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 18, 2012

N. Borenstein
Mimecast
M. Kucherawy
Cloudmark

December 16, 2011

A Reputation Vocabulary for Email Identifiers
draft-ietf-repute-email-identifiers-01

Abstract

This document defines a vocabulary for describing email identifiers (typically authors or signers) with the application/reputon media type.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on June 18, 2012.

Copyright Notice

Table of Contents

1. Introduction

This memo defines a "vocabulary" for describing reputation of an email identifier. A "vocabulary" in this context is defined in [RFCxxxx] and is used to describe assertions a reputation service provider can make about email identifiers as well as meta-data that can be included in such a reply beyond the base set specified there.

2. Terminology and Definitions

This section defines terms used in the rest of the document.

2.1. Keywords

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 [KEYWORDS].

2.2. Email Definitions

Commonly used definitions describing entities in the email architecture are defined and discussed in [EMAIL-ARCH].

2.3. Other Definitions

Other terms of importance in this memo are defined in RFCxxxx, the base memo in this document series.

3. Discussion

The expression of reputation about an email identifier requires extensions of the base set defined in [RFCxxxx]. This memo defines and registers some common assertions about an entity found in a piece of [MAIL].

3.1. Assertions

The "email-id" reputation application recognizes the following assertions:

FRAUD: The subject identifier is associated with sending or handling of fraudulent email

MALWARE: The subject identifier is associated with the sending or handling of malware via email

SPAM: The subject identifier is associated with sending or handling of unwanted bulk email

INVALID-RECIPIENTS: The subject identifier is associated with delivery attempts to nonexistent recipients

For all assertions, the RATING scale is linear: A value of 0.0 means there is no data to support the assertion, a value of 1.0 means all accumulated data support the assertion, and the intervening values have a linear relationship (i.e., a score of "x" is twice as strong of an assertion as a value of "x/2").

3.2. Vocabulary Extensions

The "email-id" reputation application recognizes the following OPTIONAL extensions to the basic vocabulary defined in [RFCxxxx]:

IDENTITY: A token indicating the source of the identifier; that is, where the subject identifier was found in the message. This MUST be one of:

DKIM: The signing domain, i.e. the value of the "d=" tag, found on a valid [DKIM] signature in the message

IPV4: The IPv4 address of the client

IPV6: The IPv6 address of the client

RFC5321.MAILFROM: The RFC5321.MailFrom value of the envelope of a message of the message (see [SMTP])

RFC5322.FROM: The RFC5322.From field of the message (see [MAIL])

SPF: The domain name portion of the identifier (RFC5321.MailFrom or RFC5321.Helo) verified by [SPF])

RATE: A token that recommends an overall message acceptance rate for the subject domain. This is expected to be a value tailored to the requesting agent; for example, the reputation service would use this to indicate that, based on the data reported by the requesting agent, the service recommends a particular message limit for that agent. The value is an unsigned decimal value.

SOURCES: A token relating a count of the number of sources of data that contributed to the reported reputation. This is in contrast to the SAMPLE-SIZE parameter, which indicates the total number of reports across all reporting sources.

A reply that does not contain the IDENTITY or SOURCES extensions is making a non-specific statement about how the reputation returned was developed. A client may use or ignore such a reply at its discretion.

4. IANA Considerations

This memo presents one action for IANA, namely the registraton of the reputation application "email-id".

4.1. Registration of 'email-id' Reputation Application

This section registers the "email-id" reputation application, as defined in [RFCxxxx+1]. The registration parameters are as folows:

- Application name: email-id

- Short description: Evaluates DNS domain names found in email identifiers

- Defining document: [this memo]

- Status: current

- Application-specific query parameters:

  subject: (current) specifies the subject of the reputation query; in this case, it is the email identifier whose reputation is requested

5. Security Considerations

This memo describes security considerations introduced by the reputation application and vocabulary defined here.

[TBD]

6. Informative References

[DKIM] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", RFC 6376, September 2011.

[EMAIL-ARCH] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

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

[MAIL] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,

October 2008.

[SPF] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

Appendix A. Acknowledgments

The authors wish to acknowledge the contributions of the following to this specification: Scott Kitterman, John Levine, Doug Otis, and David F. Skoll.

Appendix B. Public Discussion

Public discussion of this suite of memos takes place on the domainrep@ietf.org mailing list. See https://www.ietf.org/mailman/listinfo/domainrep.

Authors' Addresses

Nathaniel Borenstein
Mimecast
203 Crescent St., Suite 303
Waltham, MA 02453
USA

Phone: +1 781 996 5340
Email: nsb@guppylake.com

Murray S. Kucherawy
Cloudmark
128 King St., 2nd Floor
San Francisco, CA 94107
USA

Phone: +1 415 946 3800
Email: msk@cloudmark.com