REPUTE Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 8, 2012

N. Borenstein
Mimecast
M. Kucherawy
Cloudmark

April 6, 2012

A Reputation Response Set for Email Identifiers
draft-ietf-repute-email-identifiers-03

Abstract

This document defines a response set for describing assertions a reputation service provider can make about email identifers, for use in generating reputons.

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 October 8, 2012.

Table of Contents

1. Introduction

This document specifies a response set for describing reputation of an email identifier. A "response set" in this context is defined in [I-D.REPUTE-MODEL] 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.

An atomic reputation response is called a "reputon", also defined in that document.

2. Terminology and Definitions

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

2.1. Key Words

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 document are defined in [I-D.REPUTE-MODEL], the base document for the reputation services work.

3. Discussion

The expression of reputation about an email identifier requires extensions of the base set defined in [I-D.REPUTE-MODEL]. This document 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, such as "phishing" (some good discussion on this topic can be found in [IODEF-PHISHING])

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. Response Set Extensions

The "email-id" reputation application recognizes the following OPTIONAL extensions to the basic response set defined in [I-D.REPUTE-MODEL]:

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.HELO: The RFC5321.Helo value used by the (see [SMTP]) 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])

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 can use or ignore such a reply at its discretion.

3.3. Query Extensions

A query within this application can include the OPTIONAL query parameter "identity" to indicate which specific identity is of interest to the query. Legal values are the same as those listed in Section 3.2.

4. IANA Considerations

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

4.1. Registration of 'email-id' Reputation Application

This section registers the "email-id" reputation application, as per the IANA Considerations section of [I-D.REPUTE-MODEL]. The registration parameters are as folows:

- Application name: email-id
- Short description: Evaluates DNS domain names found in email identifiers
- Defining document: [this document]
- Status: current
- Subject: A string appropriate to the identifier of interest (see Section 3.2 of this document)
- Application-specific query parameters:

  identity: (current) as defined in Section 3.3 of this document

- Application-specific extensions:

identity: (current) as defined in Section 3.2 of this document

5. Security Considerations

This section describes security considerations introduced by the reputation application and response set extensions defined here.

[TBD]

6. References

6.1. Normative 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.

[I-D.REPUTE-MODEL] Borenstein, N. and M. Kucherawy, "A Model for Reputation Interchange", draft-ietf-repute-model (work in progress), November 2011.

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

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

6.2. Informative References

[IODEF-PHISHING] Cain, P. and D. Jevans, "Extensions to the IODEF-Document Class for Reporting Phishing", RFC 5901, July 2010.

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

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

Appendix A. Acknowledgments

The authors wish to acknowledge the contributions of the following to this specification: Scott Kitterman, John Levine, S. Moonesamy, 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