MARF Working Group
Internet-Draft
Updates: 4408 (if approved)
Intended status: Standards Track
Expires: August 31, 2012

S. Kitterman
Agari Data, Inc.

February 28, 2012

SPF Authentication Failure Reporting using the Abuse Report Format
draft-ietf-marf-spf-reporting-08

Abstract

This memo presents extensions to the Abuse Reporting Format (ARF), and Sender Policy Framework (SPF) specifications to allow for detailed reporting of message authentication failures in an on-demand fashion.

This memo updates RFC4408 by providing an IANA registry for SPF modifiers.

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 August 31, 2012.

Table of Contents

1. Introduction

[ARF] defines a message format for sending reports of abuse in the messaging infrastructure, with an eye toward automating both the generating and consumption of those reports.

[SPF] is one mechanism for message sender authentication; it is "path-based" meaning it authenticates the route that a message took from origin to destination. The output is a verified domain name that can then be subjected to some sort of evaluation process (e.g., comparison to a known-good list, submission to a reputation service, etc.).

This document extends [SPF] to add an optional reporting address and other parameters. Extension of [ARF] to add features required for the reporting of these incidents is covered in [I-D.IETF-MARF-AUTHFAILURE-REPORT] and [I-D.IETF-MARF-AS].

This document additionally creates a an IANA registry of [SPF] record modifiers to avoid modifier namespace collisions.

2. Definitions

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. Imported Definitions

The ABNF token "qp-section" is defined in [MIME].

"local-part" is defined in [MAIL].

"addr-spec" is defined in [MAIL].

3. Optional Reporting Address for SPF

There exist cases in which a domain name owner employing [SPF] for announcing sending practices may want to know when messages are received via unauthorized routing. Currently there is no such method defined in conjunction with standardized approaches such as [ARF]. Similar information can be gathered using a specially crafted [SPF] record and a special DNS server to track [SPF] record lookups.

This document defines the following optional "modifier" (as defined in Section 4.6.1 of [SPF]) to SPF records, using the form defined in that specification:

ra= Reporting Address (plain-text; OPTIONAL; no default). MUST be a local-part (see Section 3.4.1 of [MAIL]) specifying an e-mail address to which a report SHOULD be sent when mail claiming to be from this domain (see Section 2.4 of [SPF] for a description of how domains are identified for SPF checks) has failed the evaluation algorithm described in [SPF], in particular because a message arrived via an unauthorized route. To generate a complete address to which the report is sent, the verifier simply appends to this value an "@" followed by the SPF domain per paragraph 4.1 of [SPF]. ra= modifiers in a record that was reached by following an include: mechanism MUST be ignored.

ABNF:

```
spf-report-tag = %x72.61 "=" qp-section
```

rp= Requested Report Percentage (plain-text; OPTIONAL; default is "100"). The value is an integer from 0 to 100 inclusive that indicates what percentage of incidents of SPF failures, selected at random, are to cause reports to be generated. The report generator SHOULD NOT issue reports for more than the requested percentage of incidents. An exception to this might be some out-of-band arrangement between two parties to override it with some mutually agreed value. Report generators MAY make use of the "Incidents:" field in [ARF] to indicate that there are more reportable incidents than there are reports.

ABNF:

```
spf-rp-tag = %x72.69 *WSP "=" *WSP 1*12DIGIT "/" 1*12DIGIT
```

rr= Requested Reports (plain-text; OPTIONAL; default is "all"). The value MUST be a colon-separated list of tokens representing those conditions under which a report is desired. See Section 4.1 for a list of valid tags.

ABNF:

```
spf-rr-type = ( "all" / "e" / "f" / "s" / "n" )

spf-rr-tag = %x72.72 "=" spf-rr-type 0* ( ":" spf-rr-type )
```

In the absence of an "ra=" tag in the SPF record, the "rp=" and "rr=" tags MUST be ignored, and the report generator MUST NOT issue a report.

4. Requested Reports

This memo also includes, as the "rr" tokens defined above, the means by which the sender can request reports for specific circumstances of interest. Verifiers MUST NOT generate reports for incidents that do not match a requested report, and MUST ignore requests for reports not included in this list.

4.1. Requested Reports for SPF Failures

The following report requests are defined for SPF results:

all All reports are requested.

e Reports are requested for messages that produced an SPF result of "TempError" or "PermError".

f Reports are requested for messages that produced an SPF result of "Fail".

s Reports are requested for messages that produced an SPF result of "SoftFail".

n Reports are requested for messages that produced an SPF result of "Neutral" or "None".

5. IANA Considerations

As required by [IANA-CONSIDERATIONS], this section contains registry information for the new [SPF] modifiers.

5.1. SPF Modifier Registration

IANA is requested to create the Sender Policy Framework Modifier Registry, to include a list of all registered SPF modifier names and their defining documents.

New registrations or updates MUST be published in accordance with the "Specification Required" guidelines as described in [IANA-CONSIDERATIONS]. New registrations and updates MUST contain the following information:

1. Name of the modifier being registered or updated

2. The document in which the specification of the modifier is published

3. New or updated status, which MUST be one of:

   current: The field is in current use

   deprecated: The field is in current use but its use is discouraged

   historic: The field is no longer in current use

An update may make a notation on an existing registration indicating that a registered field is historic or deprecated if appropriate.

MODIFIER	REFERENCE	STATUS
exp	RFC4408	current
redirect	RFC4408	current
ra	(this document)	current
rp	(this document)	current
rr	(this document)	current

6. Security Considerations

Security issues with respect to these reports are similar to those found in [DSN].

6.1. Inherited Considerations

Implementors are advised to consider the Security Considerations sections of [SPF], [ARF], [I-D.IETF-MARF-AS], and [I-D.IETF-MARF-AUTHFAILURE-REPORT].

6.2. Additional forgery considertion

In addition to the advice in security considerations of [I-D.IETF-MARF-AS] the additional consderations apply to [SPF] auth failure reports. If the MAIL FROM command is not the NULL return address, i.e., "MAIL FROM:<>", then the selected MAIL FROM address MUST pass [SPF] MAIL FROM checks on receipt. The HELO/EHLO command SHOULD also be selected so that it will pass [SPF] HELO checks.

7. References

7.1. Normative References

[ARF] Shafranovich, Y., Levine, J., and M. Kucherawy, "An Extensible Format for Email Feedback Reports", RFC 5965, August 2010.

[I-D.IETF-MARF-AS] Falk, J. and M. Kucherawy, Ed., "Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF)", February 2012.

[I-D.IETF-MARF-AUTHFAILURE-REPORT] Fontana, H., "Authentication Failure Reporting using the Abuse Report Format", January 2012.

[IANA-CONSIDERATIONS] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008.

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

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

[MIME] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

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

7.2. Informative References

[DSN] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, January 2003.

Appendix A. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: Murray Kucherawy, Tim Draegen, Julian Mehnle, and John Levine.

Appendix B. Examples

B.1. SPF DNS record for domain that sends no mail, but requests reports

```
v=spf1 ra=postmaster -all
```

B.2. Minimal SPF DNS record change to add a reporting address

```
v=spf1 mx:example.org ra=postmaster -all
```

B.3. SPF DNS record with reporting address, report percentage, and requested report type

```
v=spf1 mx:example.org -all ra=postmaster rp=10 rr=e
```

Author's Address

Scott Kitterman
Agari Data, Inc.
3611 Scheel Dr
Ellicott City, MD 21042
US

Phone: +1 301 325 5475
Email: skitterman@agari.com