Internet Engineering Task Force (IETF)
Request for Comments: 6652
Updates: 4408
Category: Standards Track
ISSN: 2070-1721

S. Kitterman
Agari

June 2012

Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format

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 RFC 4408 by providing an IANA registry for SPF modifiers.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6652.

Table of Contents

1. Introduction

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

The Sender Policy Framework [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 [ARF-AUTHFAIL] and [ARF-AS].

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

2. Definitions

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. 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 an ADministrative Management Domain (ADMD) (see [EMAIL-ARCH]) 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-compliant domain per Section 4.1 of [SPF]. ra= modifiers in a record that was reached by following an "include" mechanism (defined in Section 5.2 of [SPF]) MUST be ignored.

ABNF:

```
spf-report-tag = "ra=" 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 = "rp=" 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 = "rr=" spf-rr-type *( ":" 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-CONS], this section contains registry information for the new [SPF] modifiers.

5.1. SPF Modifier Registration

IANA has created the Modifier Names registry under Sender Policy Framework Parameters, to include a list of all registered SPF modifier names and their defining documents.

New registrations or updates are to be published in accordance with the "Specification Required" guidelines as described in [IANA-CONS]. 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 the following:

   Current: The field is in current use

   Deprecated: The field might be 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	RFC 4408	Current
redirect	RFC 4408	Current
ra	(this document)	Current
rp	(this document)	Current
rr	(this document)	Current

6. Security Considerations

Inherited considerations: implementers are advised to consider the Security Considerations sections of [SPF], [ARF], [ARF-AS], and [ARF-AUTHFAIL].

In addition to the advice in the Security Considerations section of [ARF-AS], these additional considerations apply to the generation of [SPF] authentication failure reports:

6.1. Identity Selection

Preventing an [SPF] failure for SPF authentication failure reports is essential to mitigate the risk of data loops.

> If the [SMTP] return address to be used will not be the NULL return address, i.e., "MAIL FROM:<>", then the selected return address MUST be selected such that it will pass [SPF] MAIL FROM checks upon initial receipt.
>
> If the report is passed to the Message Submission Agent (MSA) (MSA is described in [EMAIL-ARCH] using [SMTP]), the HELO/EHLO command parameter SHOULD also be selected so that it will pass [SPF] HELO checks.

6.2. Report Volume

It is impossible to predict the volume of reports this facility will generate when enabled by a report receiver. An implementer ought to anticipate substantial volume, since the amount of abuse occurring at receivers cannot be known ahead of time, and may vary rapidly and unpredictably.

7. References

7.1. Normative References

[ABNF] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

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

[ARF-AS] Falk, J. and M. Kucherawy, Ed., "Creation and Use of Email Feedback Reports: An Applicability Statement for the Abuse Reporting Format (ARF)", RFC 6650, June 2012.

[ARF-AUTHFAIL] Fontana, H., "Authentication Failure Reporting Using the Abuse Reporting Format", RFC 6591, April 2012.

[IANA-CONS] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[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.

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

[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.

7.2. Informative References

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

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
3611 Scheel Dr.
Ellicott City, MD 21042
US

Phone: +1 301 325 5475
EMail: scott@kitterman.com