SPFBIS Working Group
Internet-Draft
Intended status: Informational
Expires: October 21, 2012

M. Kucherawy
Cloudmark

April 19, 2012

Resolution of The SPF/Sender-ID Experiment draft-ietf-spfbis-experiment-05

Abstract

In 2006 the IETF published a suite of protocol documents comprising SPF and Sender-ID, two proposed email authentication protocols. Because of possible interoperability issues, particularly but not only those created by simultaneous use of the two protocols by a receiver, the IESG was unable to determine technical consensus and decided it was best to publish all of RFC4405, RFC4406, RFC4407 and RFC4408 as Experimental documents. The IESG invited the community to observe their deployments for a period of time, and expressed hope for later convergence of opinion.

After six years, sufficient experience and evidence have been collected that the experiment thus created can be considered concluded, and a single protocol can be advanced. This document presents those findings.

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 21, 2012.

Copyright Notice

Table of Contents

1. Introduction

In April 2006, the IETF published the [SPF] and Sender-ID email authentication protocols, the latter consisting of three documents ([SUBMITTER], [SENDER-ID], and [PRA]). Both of these protocols enable one to publish via the Domain Name System a policy declaring which mail servers were authorized to send email on behalf of a specific domain name. The two protocols made use of this policy statement and some specific (but different) logic to evaluate whether the email client sending or relaying a message was authorized to do so.

Due to the absence of consensus behind one or the other, and because Sender-ID supported use of the same policy statement defined by SPF, the IESG at the time was concerned that an implementation of Sender-ID might erroneously apply that statement to a message and, depending on selected recipient actions, could improperly interfere with message delivery. As a result, the IESG required the publication of all of these documents as Experimental, and requested that the community observe deployment and operation of the protocols over a period of two years from the date of publication in order to determine a reasonable path forward. (For further details about the IESG's concern, see the IESG Note prepended to all of those documents.)

In line with the IESG's request to evaluate after a period of time, this document concludes the experiment by presenting evidence regarding both deployment and comparative effect of the two protocols. At the end it presents conclusions based on the data collected.

It is important to note that this document makes no direct technical comparison of the two protocols in terms of correctness, weaknesses, or use case coverage. The email community at large has already done that. Rather, the analysis presented here merely observes what has been deployed and supported in the time since the protocols were published, and draws conclusions based on those observations.

2. Definitions

The term "RRTYPE" is used to refer to a Domain Name System ([DNS]) Resource Record (RR) type. These are always expressed internally in software as numbers, assigned by IANA under Expert Review provisions. Assigned RRTYPEs also have names. The two of interest in this work are the TXT RRTYPE (16) and the SPF RRTYPE (99).

3. Evidence of Deployment

This section presents the collected research done to determine what parts of the two protocol suites are in general use, as well as related issues like [DNS] support.

3.1. DNS Resource Record Types

Two large-scale DNS surveys were run that looked for the two supported kinds of RRTYPEs that can contain SPF policy statements. Specifically, these surveys pulled a large number of domain names from recent activity logs and queried their nameservers for both RRTYPEs that can be used for SPF and/or Sender-ID.

DNS Survey #1

Domains queried	1,000,000	-
TXT replies	397,511	39.8%
SPF replies	6,627	<0.1%
SPF+TXT replies	6,603	<0.1%
spf2.0/* replies	5,291	<0.1%

The "spf2.0/*" replies are those replies whose payload started with the string "spf2.0/", which are express requests for Sender-ID processing.

DNS Survey #2

Domains queried	259,918	-
TXT replies	142,640	54.9%
SPF replies	2,727	1.0%
SPF+TXT replies	2,554	<0.1%
spf2.0/* replies	6,972	2.7%

During this second survey, some domains were observed to provide immediate answers for RRTYPE 16 queries, but would time out waiting for replies to RRTYPE 99 queries. For example, it was observed that 4,179 (over 1.6%) distinct domains in the survey returned a result of some kind (a record or an error) for the TXT query in time N, while the SPF query ultimately failed after at least time 4N.

DNS Survey #3

Domains queried	100,000	-
TXT replies	46,221	46.2%
SPF replies	954	<0.1%
SPF+TXT replies	1,383	1.4%

A survey was done of queries for RRTYPE 16 and RRTYPE 99 records by observing nameserver logs. Only a few queries were ever received for RRTYPE 99 records, and those almost exclusively came from one large email service provider that queried for both RRTYPEs. The vast majority of other querying agents only ever requested RRTYPE 16.

3.2. Implementations

It is likely impossible to determine from a survey which Mail Transfer Agents (MTAs) have SPF and/or Sender-ID checking enabled at message ingress since it does not appear, for example, in the reply to the EHLO command from extended [SMTP]. We therefore rely on evidence found via web searches, and observed the following:

- A web site [SID-IMPL] dedicated to highlighting Sender-ID implementations last updated in late 2007 listed 13 commercial implementations, which we assume means they implement the PRA checks. At least one of them is known no longer to be supported by its vendor. There were no free open source implementations listed.

- The [OPENSPF] web site maintains a list of implementations of SPF. At the time of this document's writing it listed six libraries, 22 MTAs with built-in SPF implementations, and numerous patches for MTAs and mail clients. The set included a mix of commercial and free open source implementations.

3.3. The SUBMITTER SMTP Extension

In a review of numerous MTAs in current or recent use, two (Santronics WinServer and McAfee MxLogic) were found to contain implementations of the SMTP SUBMITTER extension as part of the MTA service, which could act as an enabler to Sender-ID.

An unknown number of SMTP clients implement SUBMITTER. Although there is substantial activity showing its use in MTA logs, it is not possible to determine whether they are multiple instances of the same client, or separate client implementations.

An active survey was done of a approximately 170,00 running and publicly reachable MTAs. Fewer than 4.5% of these advertised the SUBMITTER extension. Based on the SMTP banner presented upon connection, the entire set of SUBMITTER-enabled MTAs consisted of the two found during the review (above) and a third whose identity could not be positively determined.

Over 97% of the responding MTAs advertising the SUBMITTER SMTP extension were different instances of one MTA. The service operating that MTA reported that about 11% of all observed SMTP sessions involved SMTP clients which make use of the SUBMITTER extension.

4. Evidence of Differences

Separate surveys compared the cases where the PRA (used by Sender-ID) and the RFC5321.MailFrom address (used by SPF) differed. The results of these tests showed that at least 50% of the time the two addresses were the same, but beyond that the percentage varied substantially from one sampling location to the next due to the nature of the mail streams they each receive.

Despite this, one working group contributor analyzed approximately 150,000 messages and found that in more than 95% of those cases, Sender-ID and SPF reach the same conclusion about a message, meaning either both protocols return a "pass" result or both return a "fail" result. The data set yielding this response could not further characterize the cases in which the answers differed.

5. Analysis

Given the six years that have passed since the publication of the experimental RFCs, and the evidence reported in the earlier sections of this document, the following analysis appears to be supported:

1. There has not been substantial adoption of the RRTYPE 99 (SPF) DNS resource record. In all large-scale surveys performed for this work, less than 2% of responding domains published RRTYPE 99 records, and almost no clients requested them.

2. Of the records retrieved, fewer than 3% requested processing of messages using the PRA algorithm, which was an essential part of Sender-ID.

3. Although the two mechanisms often used different email addresses as the subject being evaluated, no data collected showed any substantial operational benefit (e.g., cheaper processing,

improved accuracy) to using Sender-ID over SPF.

4. A review of known implementations shows significant support for both protocols, though there were more implementations in support of SPF than of Sender-ID. Further, the SPF implementations showed better upkeep and current interest than the Sender-ID implemenations.

5. A survey of running MTAs shows fewer than 5% of them advertised the SUBMITTER extension, which is a Sender-ID enabler. Only three implementations of it were found.

6. Although they may be marginal, there remain obstacles to deployment of protocols that use DNS RRTYPEs other than the most common ones, including firewalls and DNS servers that block or discard requests for unknown RRTYPEs. Further, few if any web-based DNS configuration tools offer support for RRTYPE 99 records.

6. Conclusions

It is standard procedure within the IETF to document as standard those protocols and practices that have come into sufficient common use as to become part of the basic infrastructure.

In light of the this and the analysis in the previous section, the following conclusions are supported:

1. The experiment comprising the series of RFCs defining the SUBMITTER SMTP extension, the Sender-ID mechanism, the Purported Responsible address algorithm, and SPF, should be considered concluded.

2. The absence of significant adoption of the RRTYPE 99 DNS Resource Record suggests that it has not attracted enough support to be useful.

3. The absence of significant adoption of the [SUBMITTER] extension, [SENDER-ID], and [PRA], indicates that there is not a strong community prepared to develop those mechanisms beyond experimental status.

4. Continued widespread use of [SPF] indicates it is worthy of consideration for the Standards Track.

Appendix A is offered as a cautionary review of problems that affected the process of developing SPF and Sender-ID in terms of

their use of the DNS.

7. IANA Considerations

This document presents no actions for IANA. [RFC Editor: Please remove this section prior to publication.]

8. Security Considerations

This document contains information for the community, akin to an implementation report, and does not introduce any new security concerns. Its implications could, in fact, resolve some.

9. Informative References

[DNS] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[OPENSPF] "Sender Policy Framework: Project Overview", <http://www.openspf.net>.

[PRA] Lyon, J., "Purported Responsible Address in E-Mail Messages", RFC 4407, April 2006.

[SENDER-ID] Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", RFC 4406, April 2006.

[SID-IMPL] "Sender ID Framework Industry Support and Solutions", October 2007, <http://www.microsoft.com/mscorp/safety/technologies/senderid/support.mspx>.

[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.

[SUBMITTER] Allman, E. and H. Katz, "SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message", RFC 4405, April 2006.

Appendix A. Experiences Developing SPF

SPF was originally developed by a community of interested developers outside the IETF, with the intent of bringing it to the IETF for standardization after it had become relatively mature and ready for the IETF standards track process.

At the time of SPF's initial development, the prospect of getting an RRTYPE allocated for SPF was not seriously considered, partly because doing so had high barriers to entry. As a result, at the time it was brought to the IETF for development and publication, there was already a substantial and growing installed base that had SPF running using TXT RRs. Eventually the application was made for the new RRTYPE as a result of pressure from the DNS experts in the community, who insisted upon doing so as the preferred path toward using the DNS for storing such things as policy data.

Later, after RRTYPE 99 was assigned (long after IESG approval of the document, in fact), a plan was put into place to effect a gradual transition to using RRTYPE 99 instead of using RRTYPE 16. This plan failed to take effect for four primary reasons:

1. there was hesitation to make the transition because existing nameservers (and, in fact, DNS-aware firewalls) would drop or reject requests for unknown RRTYPEs (see Section 3 for evidence of this), which means successful rollout of a new RRtype is contingent upon widespread adoption of updated nameservers and resolver functions;

2. many DNS provisioning tools (e.g., web interfaces to controlling DNS zone data) were, and still are, typically lethargic about adding support for new RRTYPEs;

3. the substantial deployed base was already using RRTYPE 16, and it was working just fine, leading to inertia;

4. [SPF] itself included a faulty transition plan, likely because of the late addition of a requirement to develop one: It said a server SHOULD publish both RRTYPEs and MUST publish at least one, while a client can query either or both, which means both can claim to be fully compliant while failing utterly to interoperate. Publication occurred without proper IETF review, so this was not detected prior to publication.

It is likely that this will happen again if the bar to creating new RRTYPEs even for experimental development purposes is not lowered, and handling of unknown RRTYPEs in software becomes generally more graceful. Also important in this regard is encouragement of support

for new RRTYPEs in DNS record provisioning tools.

There are DNS experts within the community that will undoubtedly point to DNS servers and firewalls that mistreat queries for unknown RRTYPEs, and claim they are broken, as a way of answering this concern. This is undoubtedly correct, but the reality is that they are among us and likely will be for some time, and this needs to be considered as new protocols and IETF procedures are developed.

Appendix B. Acknowledgments

The following provided operational data that contributed to the evidence presented above:

Cisco: contributed data about observed Sender-ID and SPF records in the DNS for a large number of domains

Hotmail: contributed data about the difference between RFC5321.MailFrom and RFC5322.From domains across large mail volumes, and a survey of DNS queries observed in response to outgoing mail traffic

John Levine: conducted a survey of DNS server logs to evaluate SPF-related query traffic

McAfee: provided details about their SUBMITTER implementation and usage statistics

Santronics: contributed data about the use of the SUBMITTER extension in aggregate SMTP client traffic

The Trusted Domain Project: contributed data about the difference between Sender-ID and SPF results, conducted one of the two detailed TXT/SPF RRTYPE surveys including collecting timing data, and conducted the MTA SUBMITTER survey

The author would also like to thank the following for their contributions to the development of the text in this document: Dave Crocker, Scott Kitterman, Barry Leiba, John Leslie, John Levine, Hector Santos, and Alessandro Vesely.

Author's Address

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

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