SPFBIS Working Group
Internet-Draft
Intended status: Informational
Expires: September 7, 2012

M. Kucherawy
Cloudmark

March 6, 2012

The SPF/Sender-ID Experiment
draft-kucherawy-spfbis-experiment-03

Abstract

In 2006 the IETF published a suite of protocol documents comprising SPF and Sender-ID, two proposed email authentication protocols. Because of interoperability concerns created by simultaneous use of the two protocols by a receiver, and some concerns with Sender-ID and compatibility with existing standards, the IESG required them to have Experimental status and invited the community to observe their deployments for a period of time, hoping convergence would be possible later.

After six years, sufficient experience and evidence have been collected that the experiment thus created can be considered concluded, and a common path forward can be selected. This memo presents those findings.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

In April, 2006, the IETF published the [SPF] and [SUBMITTER]/[SENDER-ID]/[PRA] email authentication protocols. Both of these enabled 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 or not the email client sending or relaying a message was authorized to do so.

Because Sender-ID could use the same policy statement as 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 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.)

Accordingly, this working group has convened to resolve this experiment and propose advancement of a single protocol going forward. This memo presents evidence on both deployment and efficacy of the two protocols, and further discusses the increasing need for consensus. At the end it presents conclusions and recommends a path forward, as the IESG requested.

2. The Need For Consensus

These two protocols fall into a family of protocols that provide domain-level email authentication services. Another prominent one is [DKIM]. Various efforts exist that use these as building blocks to increased abuse filtering capabilties, and indeed this sort of work has spawned another working group in the Applications area, with still more of these incubating in associations and trade groups outside of the IETF.

There is thus some palpable interest in having a path authorization scheme, as well as a domain-level signing scheme, on the Standards Track so that these newer technologies can develop with confidence. This is, in part, why the community has decided to expend the effort to bring this experiment to a conclusion and document the results, and then advance a single path authorization technology.

3. Evidence of Deployment

Two participants ran large-scale DNS surveys looking for SPF policy records.

One data source for this report requested SPF records from approximately 287,000 domains that had a TXT (type 16) policy record. Of these, 4,613 (1.6%) also publish SPF (type 99) resource records.

[pending: updated TDP report numbers go in here] Another source requested SPF records from 239,000 domains. Of these, # returned type 16 answers, # returned type 99 answers, # returned both types, and # returned neither. Of those answers retrieved, # included records that start with the string "spf2.0/pra" which are specific requests for Sender-ID processing by receivers.

During this second survey, some domains were observed to provide immediate answers for type 16 queries, but would time out waiting for replies to type 99 queries.

It is likely impossible to determine from a survey which 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 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.

- The [OPENSPF] web site maintains a list of known implementations of SPF. At the time of this memo's writing it listed six libraries, 22 MTAs with built-in SPF implementations, and numerous patches for MTAs and mail clients.

In a survey of numerous MTAs in current or recent use, only two (Santronics WinServer and McAfee MxLogic) were found to contain implementations of the SMTP SUBMITTER extension in server mode, which could act as an enabler to Sender-ID. An unknown number of clients implement it; although there is substantial activity showing its use in logs, it is unclear whether these are separate implementations by legitimate senders, or merely instances of distributed automated malware seeking to improve their odds of reaching the end user.

[pending: passive DNS query report from John Levine]

[pending: SPF query results from Hotmail]

[other data TBD]

4. Evidence of Differences

It is plain from inspection of the two protocols that they have much in common: For a single message, both require the same number of DNS queries, and both require the same code to parse the result. The PRA algorithm applied by Sender-ID is, however, more expensive than simply extracting the domain name from the omnipresent RFC5321.MailFrom. Thus, SPF is cheaper to apply to a message.

One set of specific data collected by a working group contributor shows that in more than 95.5% of 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.

[pending: MAIL FROM/PRA comparison report from Hotmail]

[other data TBD]

5. 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.

Given the evidence above, the working group feels that the experiment allows the following conclusions:

1. [WG conclusions here]

6. IANA Considerations

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

7. Security Considerations

This memo contains information for the community only, akin to an implementation report, and does not introduce any new security

concerns. Its implications could, in fact, resolve some.

8. Informative References

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

[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. Acknowledgments

The following provided operational data that contributed to the findings 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

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, and counts of unique domains appearing to publish different kinds of SPF and Sender-ID records

The author would also like to thank the following for their contributions to the development of this memo: Dave Crocker, and Scott Kitterman

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