MARID Working Group
Internet Draft
Document: draft-ietf-marid-submitter-01.txt

Expires: December 2004

E. Allman
Sendmail, Inc
H. Katz
Microsoft Corp

June 2004

SMTP Service Extension for Indicating the Responsible Submitter of an E-mail Message

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [STD].

Internet-Drafts are working documents of Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Copyright Notice

Abstract

This memo defines an extension to the Simple Mail Transfer Protocol SMTP) service, which allows an SMTP client to specify the responsible submitter of an e-mail message. The responsible submitter is the e-mail address of the entity most recently responsible for introducing a message into the transport stream. This extension helps receiving e-mail servers efficiently determine whether the SMTP client is authorized to transmit mail on behalf of the responsible submitter's domain.

Conventions Used in This Document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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 RFC-2119 [KEYWORDS].

Table of Contents

1. Introduction

The practice of falsifying the identity of the sender of an e-mail message, commonly called "spoofing", is a prevalent tactic used by senders of unsolicited commercial e-mail or "spam". A number of proposals have been put forward to address the spoofing problem. Notable among them are [RMX], [SPF], [LMAP] and [CALLERID].

These proposals have many key elements in common. In particular, they all describe a mechanism by which receiving e-mail servers can validate whether the client MTA is authorized to transmit e-mail messages on behalf of the sender's domain.

They differ in their choice of the identity used as a basis for the validation, that is, in their determination of the "sender" of the message. In this specification, this identity will be referred to as the "purported responsible address" of the message, that is, the Internet address from which the message purports to originate. The purported responsible domain is the domain portion of that address. [RMX], [SPF] and [LMAP] use the domain part of the e-mail address used on the RFC 2821 MAIL FROM command, and in some cases the EHLO command, as the purported responsible domain. [CALLERID] derives the purported responsible domain by examining certain RFC 2822 headers specified in the body of the message.

Each approach has certain advantages and disadvantages.

Deriving the purported responsible domain from RFC 2821 data has the advantage that validation can be performed before the SMTP client has transmitted the message body. If spoofing is detected, then the SMTP server has the opportunity, depending upon local policy, to reject the message before it is ever transmitted. The disadvantage of this approach is the risk of false positives, that is, incorrectly concluding that the sender's e-mail address has been spoofed. There are today legitimate reasons why the Internet domain names used in RFC 2821 commands may be different from that of the sender of an e-mail message.

Deriving the purported responsible domain from RFC 2822 headers has the advantage of basing the sender validation on an identity that is usually visible to the end recipient of the message. This aids in detection of a particularly noxious form of spoofing known as "phishing" in which a malicious sender attempts to fool a recipient into believing that a message originates from a firm well known to the recipient. This approach carries a lower risk of false positives since there are fewer legitimate reasons for RFC 2822 headers to differ from the true sender of the message. The disadvantage of this approach is that it does require parsing and analysis of message headers. In practice, much if not all the message body is also transmitted since the SMTP protocol described in RFC 2821 provides no mechanism to interrupt message transmission after the DATA command has been issued.

It is desirable to unify these two approaches in a way that combines the benefits of both while minimizing their respective disadvantages.

This memo describes just such a unified approach. It uses the mechanism described in [SMTP] to describe an extension to the SMTP protocol. Using this extension, an SMTP client can specify the e-mail address of the entity responsible for submitting the message to the SMTP client in a new SUBMITTER parameter of the SMTP MAIL command. SMTP servers can use this information to validate that the SMTP client is authorized to transmit e-mail on behalf of the Internet domain contained in the SUBMITTER parameter.

2. The SUBMITTER Service Extension

The following SMTP service extension is hereby defined:

(1) The name of this SMTP service extension is "Responsible Submitter";

(2) The EHLO keyword value associated with this extension is "SUBMITTER";

(3) The SUBMITTER keyword has no parameters;

(4) No additional SMTP verbs are defined by this extension;

(5) An optional parameter is added to the MAIL command using the esmtp-keyword "SUBMITTER", and is used to specify the e-mail address of the entity responsible for submitting the message for delivery;

(6) This extension is appropriate for the submission protocol [SUBMIT].

3. The SUBMITTER Keyword of the EHLO Command

An SMTP server includes the SUBMITTER keyword in its EHLO response to tell the SMTP client that the SUBMITTER service extension is supported.

The SUBMITTER keyword has no parameters.

4. The SUBMITTER Parameter of the MAIL Command

If the SMTP server supports the SUBMITTER extension, then the SMTP client MAY include the SUBMITTER parameter in MAIL commands issued during the SMTP session.

The syntax of the SUBMITTER parameter is:

```
"SUBMITTER=" Mailbox
```

where Mailbox is the ABNF [ABNF] production defined in Section 4.1.2 of [SMTP]. Characters such as SP, "+" and "=" which may occur in Mailbox but are not permitted in ESMTP parameter values MUST be encoded as "xtext" as described in section 4 of [DSN].

4.1 Setting the SUBMITTER Parameter Value

The purpose of the SUBMITTER parameter is to allow the SMTP client to indicate to the server the purported responsible address of the message directly in the RFC 2821 protocol.

Therefore, SMTP clients that support the Responsible Submitter extension SHOULD include the SUMBITTER parameter on all messages where the purported responsible address, as defined in section 4 of [SENDER-ID] differs from the MAIL FROM address.

At some future time, it is likely that use of the SUBMITTER parameter will be made MANDATORY whenever the purported responsible address differs from the MAIL FROM address.

Furthermore, clients MUST, if necessary, insert such RFC 2822 headers as defined in section 4 of [SENDER-ID] in order to ensure that the purported responsible address determined from the RFC 2822 headers matches the SUBMITTER address. In other words, SUBMIT servers supporting SUBMITTER MUST scan the RFC 2822 headers for a purported responsible address to be included in subsequent SUBMITTER parameters, unless the MUA includes the parameter itself.

A common model will be for the Mail User Agent (MUA) to transmit a message to the SUBMIT server [SUBMIT] without a SUBMITTER parameter. The SUBMIT server will then validate that the MUA is allowed to submit a message using the purported Responsible Submitter address through some external scheme, perhaps SMTP Authentication [SMTPAUTH]. The SUBMIT server, acting as an SMTP client, will then add a SUBMITTER parameter for further transmission.

Any MTA supporting the Responsible Submitter extension that redirects a message from the address listed in the RFC 2821 RCPT TO command MUST modify the message by:

(a) Determining a new purported responsible address for the message that can verifiably claim to be under the control of the MTA's domain. For example, the new purported responsible address could be the name of a forwarded address, the name of a mailing list, or a fixed name at that domain.

(b) If necessary, pre-pending a Resent-From or Resent-Sender header field to the message header containing the new purported responsible address.

(c) If the purported responsible address differs from the RFC 2821 MAIL FROM address, adding or replacing the SUBMITTER parameter with the new purported responsible address.

4.2 Processing the SUBMITTER Parameter

Receivers of e-mail messages sent with the SUBMITTER parameter SHOULD select the domain part of the SUBMITTER address value as the purported responsible domain of the message, and SHOULD perform such tests, including those defined in [SENDER-ID], as are deemed necessary to determine whether the connecting SMTP client is authorized to transmit e-mail messages on behalf of that domain.

When, at some future time, use of the SUBMITTER parameter becomes MANDATORY, SMTP servers MAY use the domain part of the MAIL FROM address as the purported responsible domain in the absence of the SUBMITTER parameter.

If the above tests indicate that the connecting SMTP client is not authorized to transmit e-mail messages on behalf of the SUBMITTER domain, the receiving SMTP server MAY reject the message using "550 5.7.1 Submitter not allowed." The receiving SMTP server MAY alternatively proceed to read the message and apply local policy.

If the receiving SMTP server allows the connecting SMTP client to transmit message data, then the server SHOULD determine the purported responsible address of the message by examining the RFC 2822 message headers as described in [SENDER-ID]. If this purported responsible address does not match the address appearing in the SUBMITTER parameter, the receiving SMTP server MUST reject the message using "550 5.7.1 Submitter does not match header."

If no address header meeting these criteria is found, the SMTP server SHOULD reject the message using "554 5.7.7 Cannot verify submitter address."

Verifying MTAs are strongly urged to validate the SUBMITTER parameter against the RFC 2822 headers; otherwise, an attacker can trivially defeat the algorithm.

4.3 Transmitting to a Non-SUBMITTER Aware SMTP Server

When an MTA receives a message with a SUBMITTER parameter and must forward it to another MTA that does not support the SUBMITTER extension, the forwarding MTA MUST transmit the message without the SUBMITTER parameter. This should involve no information loss, since the SUBMITTER parameter is required to contain information derived from the message headers.

5. Examples

This section provides examples of how the SUBMITTER parameter would be used. The following dramatis personae appear in the examples:

alice@example.com: the original sender of each e-mail message.

bob@woodgrove.example.com: the final recipient of each e-mail.

bob@alumni.almamater.edu: an email address used by Bob which he has configured to forward mail to his office account at bob@woodgrove.example.com.

alice@consolidatedmessenger.net: an e-mail account provided to Alice by her mobile e-mail network carrier.

5.1 Mail Submission

Under normal circumstances, Alice would configure her MUA to submit her message to the mail system using the SUBMIT protocol [SUBMIT]. Under most circumstances this would look like a normal, authenticated SMTP transaction. The SUBMIT server will extract her name from the RFC 2822 headers for use in the SUBMITTER parameters of subsequent transmissions of the message.

5.2 Mail Forwarding

When Alice sends a message to Bob at his alumni.almamater.edu account, the SMTP session from her SUBMIT server might look something like this:

```
S: 220 alumni.almamater.edu ESMTP server ready
C: EHLO example.com
S: 250-alumni.almamater.edu
S: 250-DSN
S: 250-AUTH
S: 250-SUBMITTER
S: 250 SIZE
C: MAIL FROM:<alice@example.com> SUBMITTER=alice@example.com
S: 250 <alice@example.com> sender ok
C: RCPT TO:<bob@alumni.almamater.edu>
S: 250 <bob@alumni.almamater.edu> recipient ok
C: DATA
S: 354 okay, send message
C: (message body goes here)
C: .
S: 250 message accepted
C: QUIT
S: 221 goodbye
```

The SUBMITTER parameter is optional in this first example because alice@example.com is the original sender of the message.

The alumni.almamater.edu MTA must now forward this message to bob@woodgrove.example.com. Since the original sender of the message is alice@example.com, the alumni.almamater.edu MTA adds the SUBMITTER parameter to indicate the forwarding address that is authorized to transmit mail via that MTA. The forwarding MTA also inserts a Resent-From header in the message body to ensure consistency of the purported responsible domain derived from the RFC 2822 headers with the SUBMITTER domain.

```
S: 220 woodgrove.example.com ESMTP server ready
C: EHLO alumni.almamater.edu
S: 250-woodgrove.example.com
```

```
      S: 250-DSN
      S: 250-AUTH
      S: 250-SUBMITTER
      S: 250 SIZE
      C: MAIL FROM:<alice@example.com>
              SUBMITTER=bob@alumni.almamater.edu
      S: 250 <alice@example.com> sender ok
      C: RCPT TO:<bob@woodgrove.example.com>
      S: 250 <bob@woodgrove.example.com> recipient ok
      C: DATA
      S: 354 okay, send message
      C: Resent-From: bob@alumni.almamater.edu
      C: Received By: ...
      C: (message body goes here)
      C: .
      S: 250 message accepted
      C: QUIT
      S: 221 goodbye
```

5.3 Mobile User

Alice is at the airport and uses her mobile e-mail device to send a message to Bob. The message travels through the carrier network provided by consolidatedmessenger.net, but Alice uses her example.com address on the From line of all her messages so that replies go to her office mailbox.

Here is an example of the SMTP session between the MTAs at consolidatedmessanger.net and alumni.almamater.edu.

```
      S: 220 alumni.almamater.edu ESMTP server ready
      C: EHLO consolidatedmessenger.net
      S: 250-alumni.almamater.edu
      S: 250-DSN
      S: 250-AUTH
      S: 250-SUBMITTER
      S: 250 SIZE
      C: MAIL FROM:<alice@example.com>
              SUBMITTER=alice@consolidatedmessenger.net
      S: 250 <alice@example.com> sender ok
      C: RCPT TO:<bob@alumni.almamater.edu>
      S: 250 <bob@alumni.almamater.edu> recipient ok
      C: DATA
      S: 354 okay, send message
      C: Sender: alice@consolidatedmessenger.net
      C: Received By: ...
      C: (message body goes here)
      C: .
      S: 250 message accepted
      C: QUIT
      S: 221 goodbye
```

Note that consolidatedmessenger.net uses the SUBMITTER parameter to designate alice@consolidatedmessenger.net as the responsible submitter for this message. Further this MTA also inserts a Sender header to ensure consistency of the purported responsible domain derived from the RFC 2822 headers with the SUBMITTER domain.

5.4 Guest E-mail Service

While on a business trip, Alice uses the broadband access facilities provided by the Exemplar Hotel to connect to the Internet and send e-mail. The hotel routes all outbound e-mail through its own SMTP server, email.exemplarhotel.com.

The SMTP session for Alice's message to Bob from the Exemplar Hotel would look like this:

```
      S: 220 alumni.almamater.edu ESMTP server ready
      C: EHLO email.exemplarhotel.com
      S: 250-alumni.almamater.edu
      S: 250-DSN
      S: 250-AUTH
      S: 250-SUBMITTER
      S: 250 SIZE
      C: MAIL FROM:<alice@example.com>
                SUBMITTER=guest.services@email.exemplarhotel.com
      S: 250 <alice@example.com> sender ok
      C: RCPT TO:<bob@alumni.almamater.edu>
      S: 250 <bob@alumni.almamater.edu> recipient ok
      C: DATA
      S: 354 okay, send message
      C: Resent-From: guest.services@email.exemplarhotel.com
      C: Received By: ...
      C: (message body goes here)
      C: .
      S: 250 message accepted
      C: QUIT
      S: 221 goodbye
```

Note that email.exemplarhotel.com uses the SUBMITTER parameter to designate a generic account guest.services@email.exemplarhotel.com as the responsible submitter address for this message. A generic account is used since Alice herself does not have an account at that domain. Further this client also inserts a Resent-From header to ensure consistency of the purported responsible domain derived from the RFC 2822 headers with the SUBMITTER domain.

6. Security Considerations

The purpose of this extension is to help deter the practice of forging or "spoofing" the address of the sender of an e-mail message.

It is, however, quite possible for an attacker to forge the value of the SUBMITTER parameter also. Therefore the presence of the SUBMITTER parameter provides, by itself, no assurance of the authenticity of the message or the sender. Rather, the SUBMITTER parameter is intended to provide additional information to receiving e-mail systems to enable then to efficiently determine the validity of the sender, and specifically, whether the SMTP client is authorized to transmit e-mail on behalf of the purported responsible sender's domain. Section 4.2 describes how receiving e-mail systems should process the SUBMITTER parameter.

This extension offers no protection against a user in one domain spoofing another user within the same domain.

7. References

7.1 Normative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[DSN] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, January 2003.

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

[MSG-FORMAT] Resnick, P., Ed., "Internet Message Format", RFC 2822, April 2001.

[SENDER-ID]   Lyon, J. and Meng Weng Wong, "MTA Authentication Records in DNS", draft-ietf-marid-core-01, June 2004.

[SUBMIT]   Gellens, R. and J. Klensin, "Message Submission", RFC 2476, December 1998.

[STD]   Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[SMTP]   Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[SMTPAUTH]   Meyers, J., "SMTP Service Extension for Authentication", RFC 2554, March 1999.

7.2 Informative References

[CALLERID]   Atkinson, B, Caller ID for E-mail, May 20, 2004, draft-atkinson-callerid-00.

[LMAP]   DeKok, A. (Ed.), Lightweight MTA Authentication Protocol (LMAP) Discussion and Applicability, November 3, 2003, draft-irtf-asrg-lmap-discussion-00.

[RMX]   Danisch, Hadmut, The RMX DNS RR and method for SMTP Sender Authorization, draft-danisch-dns-rr-smtp-03.

[SPF]   Wong, Meng Weng, Mark Lentczner, Sender Permitted From, draft-mengwong-spf-01.

8. Acknowledgments

The authors would like to thank the participants of the MARID working group and the following individuals for their comments and suggestions, which greatly improved this document:

Robert Atkinson, Simon Attwell, Jim Lyon, Bruce McMillan,
Sam Neely, Pete Resnick, Nick Shelness, Meng Weng Wong

9. Authors' Addresses

Eric Allman

Sendmail, Inc.
6425 Christie Ave, Suite 400
Emeryville, CA 94608
USA

E-mail: eric@sendmail.com

Harry Katz
Microsoft Corp.
1 Microsoft Way
Redmond, WA 98052
USA

E-mail: hkatz@microsoft.com

10. Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.