Network Working Group
Request for Comments: 4405
Category: Experimental

E. Allman
Sendmail, Inc.
H. Katz
Microsoft Corp.

April 2006

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

Status of This Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

IESG Note

The following documents (RFC 4405, RFC 4406, RFC 4407, and RFC 4408) are published simultaneously as Experimental RFCs, although there is no general technical consensus and efforts to reconcile the two approaches have failed. As such, these documents have not received full IETF review and are published "AS-IS" to document the different approaches as they were considered in the MARID working group.

The IESG takes no position about which approach is to be preferred and cautions the reader that there are serious open issues for each approach and concerns about using them in tandem. The IESG believes that documenting the different approaches does less harm than not documenting them.

Note that the Sender ID experiment may use DNS records that may have been created for the current SPF experiment or earlier versions in this set of experiments. Depending on the content of the record, this may mean that Sender-ID heuristics would be applied incorrectly to a message. Depending on the actions associated by the recipient with those heuristics, the message may not be delivered or may be discarded on receipt.

Participants relying on Sender ID experiment DNS records are warned that they may lose valid messages in this set of circumstances. Participants publishing SPF experiment DNS records should consider

the advice given in section 3.4 of RFC 4406 and may wish to publish both v=spf1 and spf2.0 records to avoid the conflict.

Participants in the Sender-ID experiment need to be aware that the way Resent-* header fields are used will result in failure to receive legitimate email when interacting with standards-compliant systems (specifically automatic forwarders which comply with the standards by not adding Resent-* headers, and systems which comply with RFC 822 but have not yet implemented RFC 2822 Resent-* semantics). It would be inappropriate to advance Sender-ID on the standards track without resolving this interoperability problem.

The community is invited to observe the success or failure of the two approaches during the two years following publication, in order that a community consensus can be reached in the future.

Abstract

This memo defines an extension to the Simple Mail Transfer Protocol (SMTP) service that 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.

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". This form of abuse has highlighted the need to improve identification of the "responsible submitter" of an e-mail message.

In this specification, the responsible submitter is the entity most recently responsible for injecting a message into the e-mail transport stream. The e-mail address of the responsible submitter will be referred to as the Purported Responsible Address (PRA) of the message. The Purported Responsible Domain (PRD) is the domain portion of that address.

This specification codifies rules for encoding the purported responsible address into the SMTP transport protocol. This will permit receiving SMTP servers to efficiently validate whether or not the SMTP client is authorized to transmit mail on behalf of the responsible submitter's domain.

Broadly speaking, there are two possible approaches for determining the purported responsible address: either from RFC 2821 [SMTP] protocol data or from RFC 2822 [MSG-FORMAT] message headers. 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 those of the sender of an e-mail message.

Deriving the purported responsible domain from RFC 2822 headers has the advantage that validation can usually be based on an identity that is displayed to recipients by existing Mail User Agents (MUAs) as the sender's identity. 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 an entity 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 specification 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 most recently 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.

1.1. 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].

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

The syntax of the SUBMITTER parameter is

"SUBMITTER=" Mailbox

where Mailbox is the Augmented Backus-Naur Form (ABNF) [ABNF] production defined in Section 4.1.2 of [SMTP]. Characters such as SP, "+", and "=" that 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 MUST include the SUBMITTER parameter on all messages. This includes messages containing a null reverse-path in the MAIL command.

SMTP clients MUST set the SUBMITTER parameter value to the purported responsible address of the message as defined in [PRA]. This also applies to messages containing a null reverse-path.

In some circumstances, described in Section 7 of [SENDER-ID], SMTP clients may need to add RFC 2822 headers to the message in order to ensure that the correct SUBMITTER parameter value can be set.

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.

If these 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 SHOULD reject the message and when rejecting MUST use "550 5.7.1 Submitter not allowed."

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 [PRA]. If this purported responsible address does not match the address appearing in the SUBMITTER parameter, the receiving SMTP server MUST reject the message and when rejecting MUST use "550 5.7.1 Submitter does not match header."

If no purported responsible address is found according to the procedure defined in [PRA], the SMTP server SHOULD reject the message and when rejecting MUST use "554 5.7.7 Cannot verify submitter address."

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

Note that the presence of the SUBMITTER parameter on the MAIL command MUST NOT change the effective reverse-path of a message. Any delivery status notifications must be sent to the reverse-path, if one exists, as per Section 3.7 of [SMTP] regardless of the presence of a SUBMITTER parameter. If the reverse-path is null, delivery status notifications MUST NOT be sent to the SUBMITTER address.

Likewise, the SUBMITTER parameter MUST NOT change the effective reply address of a message. Replies MUST be sent to the From address or the Reply-To address, if present, as described in Section 3.6.2 of [MSG-FORMAT] regardless of the presence of a SUBMITTER parameter.

4.3. Transmitting to a Non-SUBMITTER-Aware SMTP Server

Notwithstanding the provisions of Section 4.1 above, when an MTA transmits a message 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@company.com.example: the final recipient of each e-mail.

bob@almamater.edu.example: an e-mail address used by Bob that he has configured to forward mail to his office account at bob@company.com.example.

alice@mobile.net.example: 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]. The MUA would transmit the message without the SUBMITTER parameter. The SUBMIT server would validate that the MUA is allowed to submit a message through some external scheme, perhaps SMTP Authentication [SMTPAUTH]. Under most circumstances, this would look like a normal, authenticated SMTP transaction. The SUBMIT server would 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 almamater.edu.example account, the SMTP session from her SUBMIT server might look something like this:

```
S: 220 almamater.edu.example ESMTP server ready
C: EHLO example.com
S: 250-almamater.edu.example
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@almamater.edu.example>
S: 250 <bob@almamater.edu.example> 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 almamater.edu.example MTA must now forward this message to bob@company.com.example. Although the original sender of the message is alice@example.com, Alice is not responsible for this most recent retransmission of the message. That role is filled by bob@almamater.edu.example, who established the forwarding of mail to bob@company.com.example. Therefore, the almamater.edu.example MTA determines a new purported responsible address for the message, namely, bob@almamater.edu.example, and sets the SUBMITTER parameter accordingly. The forwarding MTA also inserts a Resent-From header in the message body to ensure the purported responsible address derived from the RFC 2822 headers matches the SUBMITTER address.

```
S: 220 company.com.example ESMTP server ready
C: EHLO almamater.edu.example
S: 250-company.com.example
S: 250-DSN
S: 250-AUTH
S: 250-SUBMITTER
S: 250 SIZE
C: MAIL FROM:<alice@example.com>
       SUBMITTER=bob@almamater.edu.example
S: 250 <alice@example.com> sender ok
C: RCPT TO:<bob@company.com.example>
S: 250 <bob@company.com.example> recipient ok
C: DATA
S: 354 okay, send message
C: Resent-From: bob@almamater.edu.example
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 mobile.net.example, 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 mobile.net.example and almamater.edu.example.

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

Note that mobile.net.example uses the SUBMITTER parameter to designate alice@mobile.net.example as the responsible submitter for this message. Further, this MTA also inserts a Sender header to ensure the purported responsible address derived from the RFC 2822 headers matches the SUBMITTER address.

Likewise, conventional ISPs may also choose to use the SUBMITTER parameter to designate as the responsible submitter the user's address on the ISP's network if that address is different from the MAIL FROM address. This may be especially useful for ISPs that host multiple domains or otherwise share MTAs among multiple domains.

When the message is subsequently forwarded by the almamater.edu.example MTA, that MTA will replace the SUBMITTER parameter with bob@almamater.edu.example as in Section 5.2 and add its own Resent-From header.

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.hotel.com.example.

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

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

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

As before, when the message is subsequently forwarded by the almamater.edu.example MTA, that MTA will replace the SUBMITTER parameter with bob@almamater.edu.example as in Section 5.2 and add its own Resent-From header.

5.5. SUBMITTER Used on a Non-Delivery Report

Alice sends an incorrectly addressed e-mail message and receives a non-delivery report from a SUBMITTER-compliant server.

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

6. Security Considerations

This extension provides an optimization to allow an SMTP client to identify the responsible submitter of an e-mail message in the SMTP protocol, and to enable SMTP servers to perform efficient validation of that identity before the message contents are transmitted.

It is, however, quite possible for an attacker to forge the value of the SUBMITTER parameter. Furthermore, it is possible for an attacker to transmit an e-mail message whose SUBMITTER parameter does not match the purported responsible address of the message as derived from the RFC 2822 headers. Therefore, the presence of the SUBMITTER parameter provides, by itself, no assurance of the authenticity of the message or the responsible submitter. Rather, the SUBMITTER parameter is intended to provide additional information to receiving e-mail systems to enable them to efficiently determine the validity of the responsible submitter, and specifically, whether the SMTP client is authorized to transmit e-mail on behalf of the purported responsible submitter's domain. Section 4.2 describes how receiving e-mail systems should process the SUBMITTER parameter.

7. Acknowledgements

The idea of an ESMTP extension to convey the identity of the responsible sender of an e-mail message has many progenitors. Nick Shelness suggested the idea in a private conversation with one of the authors. Pete Resnick suggested a variant on the MARID mailing list. The idea was also discussed on the Anti-Spam Research Group (ASRG) mailing list.

The authors would also 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, Roy Badami, Greg Connor, Dave Crocker, Matthew Elvey, Tony Finch, Ned Freed, Mark Lentczner, Jim Lyon, Bruce McMillan, Sam Neely, Daryl Odnert, Margaret Olson, Pete Resnick, Hector Santos, Nick Shelness, Rand Wacker, and Meng Weng Wong.

8. IANA Considerations

The IANA has registered the SUBMITTER SMTP service extension.

9. References

9.1. Normative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[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., "Internet Message Format", RFC 2822, April 2001.

[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.

[SUBMIT] Gellens, R. and J. Klensin, "Message Submission for Mail", RFC 4409, April 2006.

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

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

Authors' Addresses

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

EMail: eric@sendmail.com

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

EMail: hkatz@microsoft.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).