Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 3, 2014

W. Mills
Yahoo! Inc.
M. Kucherawy
Facebook, Inc.

August 2, 2013

The Require-Recipient-Valid-Since Header Field
draft-wmills-rrvs-header-field-01

Abstract

This document defines an email header field, Require-Recipient-Valid-Since, to provide a method for senders to indicate to receivers the time when the sender last confirmed the ownership of the target mailbox. This can be used to detect changes of mailbox ownership, and thus prevent mail from being delivered to the wrong party.

The intended use of this header field is on automatically generated messages that might contain sensitive information.

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 February 3, 2014.

Copyright Notice

Table of Contents

1. Introduction 3
2. Definitions 3
3. Description 3
4. Use with Mailing Lists 5
5. Discussion 5
6. Continuous Ownership 6
7. Example 7
8. Security Considerations 7
9. Privacy Considerations 8
10. IANA Considerations 8
10.1. Header Field Registration 8
10.2. Enhanced Status Code Registration 9
11. References 9
11.1. Normative References 9
11.2. Informative References 9
Appendix A. Acknowledgments 10

1. Introduction

Mailbox Service Providers (MSPs) are public, often free, services that provide email sending and receiving capabilities to users. Some of them have policies that allow for expiration of account names when they have been unused for a protracted period. If an expired account name can be reclaimed, there is a risk of delivery of mail to the wrong party if some message author is unaware of this change of ownership.

This document defines a header field called Require-Recipient-Valid-Since. The content of this header field includes an intended recipient mailbox and a timestamp indicating at what point in time the message author believed that mailbox to be under confirmed ownership of a specific party. If the receiving system observes this field and can determine that the intended recipient mailbox has changed ownership since the provided timestamp, it can decline delivery, preventing possible misdelivery of mail.

The primary application is automatically generated messages rather than user-authored content.

2. Definitions

For a description of the email architecture, consult [EMAIL-ARCH].

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].

3. Description

The Require-Recipient-Valid-Since header field includes an intended recipient coupled with a timestamp indicating the most recent date and time when the message author believed the destination mailbox to be under the continuous ownership (see Section 6) of a specific party. Presumably there has been some confirmation process applied to establish this ownership; however, the method of making such determinations is a local matter and outside the scope of this document.

The general constraints on syntax and placement of header fields in a message are defined in Internet Message Format [MAIL].

Using Augmented Backus-Naur Form [ABNF], the syntax for the field is:

```
rrvs = "Require-Recipient-Valid-Since:" mailbox; date-time CRLF
```

"CFWS" is defined in Section 3.2.2, "date-time" is defined in Section 3.3, and "mailbox" is defined in Section 3.4, of [MAIL].

A receiving system that implements this specification determines whether the named mailbox is based at that receiving system, is a current intended recipient of the message, and has been under continuous ownership since the specified date. If that address does not match an intended local recipient (in terms of the email transaction details), the header field is ignored. Otherwise, if continuous ownership since the indicated time can be established, the message is delivered normally; if not, the message is rejected. Finally, when delivery is being performed (and the message is not being forwarded), the header field is removed. Expressed algorithmically:

1. Extract the set of Require-Recipient-Valid-Since fields from the message.

2. Discard any such fields that are syntactically invalid.

3. Discard any such fields that name a role account as listed in Mailbox Names For Common Services, Roles And Functions [ROLES].

4. Discard any such fields for which the "mailbox" portion does not match a current recipient, as listed in the RCPT TO commands in the corresponding Simple Mail Transfer Protocol [SMTP] session.

5. For each field remaining, determine if the named mailbox has been under continuous ownership since the corresponding timestamp. If it has not, reject the message.

6. RECOMMENDED: If local delivery is being performed, remove all instances of this field prior to delivery to a mailbox; if the message is being forwarded, remove those instances of this header field that were not discarded by steps 1-4 above.

The final step is not mandatory as not all mail handling agents are capable of stripping away header fields.

It is preferred that the rejection be enacted as an error response to the SMTP command verb, but this is not strictly necessary. When performing the "DATA" rejection, servers use an SMTP error code (and Enhanced Mail System Status Code [ESC], if supported) as described in Section 10.2.

Implementation is expected to be transparent to non participants, since they would typically ignore this header field.

This header field SHOULD NOT be added to a message that is addressed to multiple recipients. Because of the nature of SMTP, a message bearing this header field for multiple mailboxes could result in a single delivery attempt for multiple recipients (in particular, if two of the recipients are handled by the same server), and if any one of them fails the test, the delivery fails to all of them. It is presumed that an author making use of this field is seeking to protect transactional or otherwise sensitive data intended for a single recipient, and thus generating independent messages for each individual recipient is RECOMMENDED.

If the agent generating the message uses any kind of message authentication technology, the authentication SHOULD cover this header field. An agent receiving a message bearing this header field that is covered by some kind of authentication SHOULD ignore it if the authentication does not succeed.

To further obscure account details on the receiving system, the receiver SHOULD ignore the header field if the address within it has had one continuous owner since it was created, regardless of the purported confirmation date of the address. This is further discussed in Section 8.

4. Use with Mailing Lists

Mailing list services can store the timestamp at which a subscriber was added to a mailing list. Thus, when generating a message for distribution, the list service can use this field as a means of preventing mailing list traffic from going to the wrong recipient, and instead remove that address from further distribution.

A mailing list service that receives a message containing this field removes it from the message prior to redistributing it, limiting exposure of information regarding the relationship between the message's author and mailing list.

5. Discussion

It can be argued that the architecturally better decision would be to introduce this capability as an extension to SMTP. The exchange of meta data about the target mailbox is not part of the actual message content, nor is it meta data about the content. However, if the author and the target mailbox are separated by an SMTP server that does not implement the SMTP extension, the check will not be able to propagate to the intended receiving system. Implementing this service as a header field allows the check to occur even across non-participating systems, effectively tunneling the request.

The presence of the intended mailbox in the field content supports the case where a message bearing this header field is forwarded. The specific use case is as follows:

1. A user subscribes to a service "S" on date "D" and confirms an email address at the user's current location, "A";

2. At some later date, the user intends to leave the current location, and thus creates a new mailbox elsewhere, at "B";

3. The user replaces mailbox "A" with forwarding to "B";

4. "S" constructs a message to "A" claiming that address was valid at date "D" and sends it to "A";

5. The receiving MTA at "A" determines that the forwarding in effect was created by the same party that owned the mailbox there, and thus concludes the continuous ownership test has been satisfied;

6. If possible, "A" removes this header field from the message, and in either case, forwards it to "B";

7. On receipt at "B", either the header field has been removed, or the header field does not refer to a current envelope recipient, and in either case delivers the message.

Some services generate messages with an RFC5322.To field that does not contain a valid address, in order to obscure the intended recipient. For this reason, the original intended recipient is included in this header field.

6. Continuous Ownership

Determining continuous ownership of a mailbox is entirely a local matter. In particular, the only possible answers to that question are "yes", "no", and "unknown"; the action to be taken in the "unknown" case is a matter of local policy.

For example, when control of a domain name is transferred, the new domain owner may be unable to determine whether the owner of the subject mailbox has been under continuous ownership since the stated date if the mailbox history is not also transferred (or was not previously maintained).

It will also be "unknown" if whatever database contains mailbox ownership data is temporarily unavailable at the time a message arrives for delivery. In this case, typical SMTP temporary failure handling is appropriate.

7. Example

In the following example, "C:" indicates data sent by an SMTP client, and "S:" indicates responses by the SMTP server. Message content is CRLF terminated, though these are omitted here for ease of reading.

```
  C: [connection established]
  S: 220 server.example.com ESMTP ready
  C: HELO client.example.net
  S: 250 server.example.com
  C: MAIL FROM:<sender@example.net>
  S: 250 OK
  C: RCPT TO:<receiver@example.com>
  S: 250 OK
  C: DATA
  S: 354 Ready for message content
  C: From: Mister Sender <sender@example.net>
     To: Miss Receiver <receiver@example.com>
     Subject: Are you still there?
     Date: Fri, 28 Jun 2013 18:01:01 +0200
     Require-Recipient-Valid-Since: receiver@example.com;
       Sat, 1 Jun 2013 09:23:01 -0700

     Are you still there?
     .
  S: 550 5.7.15 receiver@example.com is no longer valid
  C: QUIT
  S: 221 So long!
```

8. Security Considerations

The response of a server implementing this protocol can disclose information about the age of existing email mailbox. Implementation of countermeasures against probing attacks is advised. For example, an operator could track appearance of this field with respect to a particular mailbox and observe the timestamps being submitted for testing; if it appears a variety of timestamps is being tried against a single mailbox in short order, the field could be ignored and the message silently discarded. This concern is discussed further in Section 9.

If the mailbox named in the field is known to have had only a single continuous owner since creation, or not to have existed at all (under any owner) prior to the date specified in the field, then the field can be silently ignored and normal message handling applied so that this information is not disclosed. Such fields are likely the product of either an attack or gross error.

9. Privacy Considerations

As described above, use of this header field in probing attacks can disclose information about the history of the mailbox. In the terminology defined in Privacy Considerations for Internet Protocols [PRIVACY], this is an Item of Interest. The harm that can be done by leaking any kind of private information varies widely and cannot be predicted, so it is prudent to be sensitive to this sort of disclosure, either inadvertently or in response to probing by an attacker. It bears restating, then, that implementing countermeasures to abuse of this capability needs strong consideration.

That some MSPs allow for expiration of account names when they have been unused for a protracted period forces a choice between two potential types of privacy vulnerabilities, one of which presents significantly greater threats to users than the other. Automatically generated mail is often used to convey authentication credentials that can potentially provide access to extremely sensitive information. Supplying such credentials to the wrong party after a mailbox ownership change could allow the previous owner's data to be exposed without his or her authorization or knowledge. In contrast, the information that may be exposed to a third party via the proposal in this document is limited to information about the mailbox history. Given that MSPs have chosen to allow transfers of mailbox ownership without the prior owner's involvement, the information leakage from the header field specified here creates far fewer risks than the potential for delivering mail to the wrong party.

10. IANA Considerations

10.1. Header Field Registration

IANA is requested to add the following entry to the Permanent Message Header Field registry, as per the procedure found in [IANA-HEADERS]:

Header field name: Require-Recipient-Valid-Since
Applicable protocol: mail ([MAIL])
Status: Standard
Author/Change controller: IETF
Specification document(s): [this document]
Related information:
Requesting review of any proposed changes and additions to this field is recommended.

10.2. Enhanced Status Code Registration

IANA is requested to register the following in the SMTP Enhanced Status Codes registry:

Code:	X.7.15
Sample Text:	Mailbox owner has changed
Associated basic status code:	5
Description:	This status code is returned when a message is received with a Require-Recipient-Valid-Since field and the receiving system is able to determine that the intended recipient mailbox has not been under continuous ownership since the specified date.
Reference:	[this document]
Submitter:	M. Kucherawy
Change controller:	IESG

11. References

11.1. Normative References

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

[IANA-HEADERS] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

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

[MAIL] Resnick, P., "Internet Message Format", RFC 5322, October 2008.

[ROLES] Crocker, D., "Mailbox Names For Common Services, Roles And Functions", RFC 2142, May 1997.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

11.2. Informative References

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

[ESC] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, January 2003.

[PRIVACY] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

Appendix A. Acknowledgments

Erling Ellingsen proposed the idea.

Reviews and comments were provided by Michael Adkins, Kurt Andersen, Alissa Cooper, Ned Freed, John Levine, Gregg Stefancik, Ed Zayas, (others)

Authors' Addresses

William J. Mills
Yahoo! Inc.

EMail: wmills_92105@yahoo.com

Murray S. Kucherawy
Facebook, Inc.
1 Hacker Way
Menlo Park, CA 94025
USA

EMail: msk@fb.com