Internet Engineering Task Force (IETF)
Request for Comments: 6212
Category: Standards Track
ISSN: 2070-1721

M. Kucherawy
Cloudmark, Inc.

April 2011

Authentication-Results Registration for Vouch by Reference Results

Abstract

This memo updates the registry of properties in Authentication-Results: message header fields to allow relaying of the results of a Vouch By Reference query.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6212.

Table of Contents

1. Introduction

[AUTHRES] defined a new header field for electronic mail messages that presents the results of a message authentication effort in a machine-readable format. In the interim, a proposal for rudimentary domain-level reputation assessment, called Vouch By Reference, [VBR] was published and is now beginning to see popular use.

This memo thus registers an additional reporting property allowing a VBR result to be relayed as an annotation in a message header.

2. Keywords

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. Discussion

Vouch By Reference [VBR] introduced a mechanism by which a message receiver can query a "vouching" service to determine whether or not a trusted third party is willing to state that mail from a particular source can be considered legitimate. When this assessment is done at an inbound border mail gateway, it would be useful to relay the result of that assessment to internal mail entities such as filters or user agents.

Reactions to the information contained in an Authentication-Results header field that contains VBR (or any) results are not specified here, as they are entirely a matter of local policy at the receiver.

4. Definition

This memo adds to the "Email Authentication Methods" registry, created by IANA upon publication of [AUTHRES], the following:

- The method "vbr"; and
- Associated with that method, the properties (reporting items) "header.md" and "header.mv".

If "header.md" is present, its value MUST be the DNS domain name about which a VBR query was made. If "header.mv" is present, its value MUST be the DNS domain name that was queried as the potential voucher for the "header.md" domain.

If the VBR query was made based on the content of a "VBR-Info" header field present on an incoming message, "header.md" is typically taken from the "md" tag of the "VBR-Info" header field, and "header.mv" is typically one of the values of the "mv" tag in the "VBR-Info" header field on that message. However, [VBR] permits a different mechanism for selection of the subject domain and/or list of vouchers, ignoring those present in any "VBR-Info" header field the message might have included. A server could even conduct a VBR query when no "VBR-Info" field was present, based on locally configured policy options. Where such mechanisms are applied, the verifying server MAY generate an Authentication-Results field to relay the results of the VBR query.

This memo also adds to the "Email Authentication Result Names" registry the following result codes and definitions:

none: No valid VBR-Info header was found in the message, or a domain name to be queried could not be determined.

pass: A VBR query was completed, and the vouching service queried gave a positive response.

fail: A VBR query was completed, and the vouching service queried did not give a positive response, or the message contained multiple VBR-Info header fields with different "mc" values (see [VBR]).

temperror: A VBR query was attempted but could not be completed due to some error that is likely transient in nature, such as a temporary DNS error. A later attempt may produce a final result.

permerror: A VBR query was attempted but could not be completed due to some error that is likely not transient in nature, such as a permanent DNS error. A later attempt is unlikely to produce a final result.

5. IANA Considerations

Per [IANA], the following items have been added to the "Email Authentication Methods" registry:

Method	Defined	ptype	property	value
vbr	RFC 6212	header	md	DNS domain name used as the subject of a VBR query
vbr	RFC 6212	header	mv	DNS domain name of the entity acting as the voucher

Also, the following items have been added to the "Email Authentication Result Names" registry:

Code	Existing/New	Defined In	Method	Meaning
none	existing	RFC 5451	vbr (added)	Section 4 of RFC 6212
pass	existing	RFC 5451	vbr (added)	Section 4 of RFC 6212
fail	existing	RFC 5451	vbr (added)	Section 4 of RFC 6212
temperror	existing	RFC 5451	vbr (added)	Section 4 of RFC 6212
permerror	existing	RFC 5451	vbr (added)	Section 4 of RFC 6212

6. Security Considerations

This memo creates a mechanism for relaying [VBR] results using the structure already defined by [AUTHRES]. The Security Considerations sections of those documents should be consulted.

7. References

7.1. Normative References

[AUTHRES] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 5451, April 2009.

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

[VBR] Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference", RFC 5518, April 2009.

7.2. Informative References

[IANA] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Appendix A. Authentication-Results Examples

This section presents an example of the use of this new header field to indicate VBR results.

A.1. VBR Results

A message that triggered a VBR query, returning a result:

```
Authentication-Results: mail-router.example.net;
      dkim=pass (good signature) header.d=newyork.example.com
            header.b=oINEO8hg;
      vbr=pass (voucher.example.net)
            header.md=newyork.example.com
            header.mv=voucher.example.org
Received: from newyork.example.com
          (newyork.example.com [192.0.2.250])
      by mail-router.example.net (8.11.6/8.11.6)
          for <recipient@example.net>
          with ESMTP id i7PK0sH7021929;
      Fri, Feb 15 2002 17:19:22 -0800
DKIM-Signature: v=1; a=rsa-sha256; s=rashani;
      d=newyork.example.com;
      t=1188964191; c=relaxed/simple;
      h=From:Date:To:VBR-Info:Message-Id:Subject;
      bh=sEu28nfs9fuZGD/pSr7ANysbY3jtdaQ3Xv9xPQtS0m7=;
      b=oINEO8hgn/gnunsg ... 9n9ODSNFSDij3=
From: sender@newyork.example.com
Date: Fri, Feb 15 2002 16:54:30 -0800
To: meetings@example.net
VBR-Info: md=newyork.example.com; mc=list;
      mv=voucher.example.org
Message-Id: <12345.abc@newyork.example.com>
Subject: here’s a sample
```

Example 1: Header Field Reporting Results from a VBR Query

Here we see an example of a message that was signed using DomainKeys Identified Mail (DKIM) and that also included a VBR-Info header field. On receipt, it is found that the "md=" field in the latter and the "d=" field in the former matched, and also that the DKIM signature verified, so a VBR query was performed. The vouching service, voucher.example.org, indicated that the sender can be trusted, so a "pass" result is included in the Authentication-Results field affixed prior to delivery.

Appendix B. Acknowledgements

The author wishes to acknowledge the following for their review and constructive criticism of this proposal: JD Falk, John Levine, and Alessandro Vesely.

Author's Address

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

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