Network Working Group	J. Levine	
Internet-Draft	Taughannock Networks	
Updates: 5518 (if approved)	June 21, 2010	
Intended status: Standards Track		
Expires: December 23, 2010		

TOC

Discard by Reference
draft-levine-dbr-00

Abstract

Domains can authenticate their outgoing mail using DKIM or other techniques. In some cases where miscreants frequently use a domain without authorization in the Author address in e-mail messages, it may be prudent for recipient mail systems to discard unauthenticated mail as likely to be fraudulent. This specification defines an extension to Vouch by Reference (VBR) that allows a certifier to identify such domains, and that recipients can use either in conjunction with or independently of VBR.

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 December 23, 2010.

Copyright Notice

from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

---

1. Introduction

TOC

Vouch by Reference (Hoffman, P., Levine, J., and A. Hathcock, “Vouch By Reference,” April 2009.) [RFC5518] allows a third party certifier to certify the owner of a domain name that is associated with received mail. In typical usage, a recipient uses VBR to identify mail from known reliable senders so it can can bypass spam filters.
A few domains, such as those of banks and online greeting cards, are frequently used without authorization in unwanted "phish" messages, intended to trick recipients into revealing personal information, to render messages that include malware installers, or other undesirable actions. If a domain can authenticate all of its outgoing mail using DKIM (Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, “DomainKeys Identified Mail (DKIM) Signatures,” May 2007.) [RFC4871] or other means, any unsigned message is likely to be unauthorized, give or take the possibility that a legitimate message could fail authentication due to the known shortcomings of authentication systems. For a limited number of domains, if the domain is indeed frequently used without authorization, the domain does authenticate all its mail, its mail is likely to be received in ways that don't make authentication fail, and the cost of losing a

legitimate message is relatively low, the overall harm to recipients could be minimized by discarding unauthenticated messages.
Since they are already evaluating the domains' practices, third party certifiers are well positioned to evaluate the suitability of domains for a policy of discarding unauthenticated messages. This document specifies a method for publishing discard advice as an extension to VBR.

> **Requirements Notation:** 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 [RFC2119] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.)

---

2. Author Domain Identity and Authentication

TOC

Although an e-mail message potentially is associated with a variety of domains, this specification imports the term Author Domain from Section 2 of ADSP (Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)," August 2009.) [RFC5617]. The identity on which the discard advice is based is the Author Domain.
Section 7 of VBR (Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference," April 2009.) [RFC5518] specifies the methods that a recipient can use to obtain an accountable domain for a message, for use with VBR. If a message has an accountable domain that is the same as the Author Domain, the message is Author Authenticated. If there is no such accountable domain, the message is not Author Authenticated.

---

3. Publication of Discard Advice

TOC

Section 5 of VBR (Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference," April 2009.) [RFC5518] specifies the DNS query to look up the certification status of a domain. This specification extends the semantics of that query to include a check for discard advice. If, for example, a message had an Author Domain of somebank.example, and a certifier's domain were certifier-a.example, the recipient would make a DNS query for a TXT record at:
somebank.example._vouch.certifier-a.example
(Note that the Author Domain may or may not be the same domain as a VBR accountable domain for the message.)
Section 6 of VBR (Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference," April 2009.) [RFC5518] specifies the types of message

content that a certifier can vouch for, as a space-separated list of lower case text strings placed in the TXT record. The discard advice is also placed in the same text record as lower case strings. The strings for types of message content are disjoint from those for discard advice, and VBR clients MUST ignore unknown strings, so the contents of the TXT records remain unambiguous, and usable by pure VBR clients.

3.1. Terms for discard advice

TOC

This specification defines the following string for discard advice.

> **discardable -** Discard the message if it is not Author Authenticated.

---

4. Checking for Discard Advice

TOC

A receiver performs the following steps:

1. Extract the Author Domain from the message.

2. Check to see whether the message is Author Authenticated. If it is, stop. The advice for Author Authenticated messages is always not to discard them.

3. It the message is not Author Authenticated, fetch the VBR record for the Author Domain for the desired certifier, as described in Section 3 (Publication of Discard Advice). If the DNS lookup fails (NXDOMAIN or NODATA status in the DNS response), stop. The certifier offers no discard advice for the domain.

4. Check the TXT record for the terms in Section 3.1 (Terms for discard advice). If the record includes "discardable", the advice is to discard the message.

---

5. Certifier Considerations

TOC

5.1. What Domains are Appropriate for Discard Advice

TOC

A certifier should only publish advice to discard a domain's mail after careful analysis, since doing so increases the risk that a valid message will not be delivered to a recipient that desired to receive it.

Is all of the domain's mail sent directly from the domain's own servers? If mail can legitmately be sent any other way, it is likely that there will be legitimate mail that is not authenticated. Common situations where mail is sent from other servers include roaming users sending through hotel networks, users who consolidate multiple mailboxes using a Web mail system, and mail sent through mailing lists.

Does the domain have individual users composing messages by hand, or is all of the mail generated by software? Experience suggests that individual users are far more likely to send legitmate mail that is not authenticated.

Is all of the domain's mail transactional notifications? For some domains, all mail reports the status of an account or transaction, such as "we shipped your order" or "your bank statement is available." These messages typically direct the recipient to look at a Web site with complete information about the transaction or account. The risk from discarding mail from these domains is relatively limited. Since the intended recipient can always recover the information in a lost message by visiting the Web site, no information is lost, just delayed, if a message is not received.

Is the domain a significant phishing target? Some domains appear in e-mail without authorization far more often than others. If a domain rarely appears in e-mail without authorization in the first place, it is relatively unlikely that an unsigned message is fraudulent rather than being a legitimate message. In that case it would be unwise to discard unsigned messages, since those messages are likely to be legitimate. On the other hand, if a domain is used without authorization in large numbers of messages, it is much more likely that an unsigned message is fraudulent.

5.2. Selection of Authentication Methods

TOC

A certifier SHOULD document the authentication method or methods that it expects to be used by the domains for which it publishes discard advice. Recipients SHOULD interpret discard advice relative to those methods. If a certifer documents more than one method, such as DK and DKIM, Author Authenticated mail can be authenticated by any of those methods. (This could be the case if a domain were migrating from DomainKeys to DKIM, and signs some of its mail with one and some with the other.

5.3. Certification and Discard Advice for the Same Domain

TOC

A certifier may wish to certify a domain's mail, and also publish discard advice for that domain. A likely example would be a financial organization that sends authenticated transactional mail, and is also a major phishing target. In that case, the certifier vouches for the domain's authenticated mail, and advises recipients to discard unauthenticated mail. The certifier's VBR record for that domain would contain:

transaction discardable

Note the recipients can use only the certification, only the discard advice, or both.

6. Receiver Considerations

TOC

The steps for checking discard advice and for checking VBR certification are different, even though a receiver may do both for the same message, and fetch the same VBR record from the DNS for both. Most notably, while receivers only do VBR checks for messages that contain a VBR-Info header field, they need to make discard advice checks for any message that is not Author Authenticated, since it is unlikely that miscreants will add VBR-Info header fields.

7. IANA Considerations

TOC

This document makes no requests to IANA.

8. Security Considerations

TOC

Discarding any incoming mail introduces a risk of losing legitimate messages. A mail system that uses discard advice should carefully weigh the relative risk of lost messages against that of delivering mail containing phishes or malware.

VBR and discard advice by their design delegate part of a mail system's management to a third party, with the risk of mishandling mail if the third party is incompetent or malicious. Before making such a delegation, a system's management SHOULD satisify itself that the third party's advice is of acceptable quality.

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC4871]	Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures," RFC 4871, May 2007 (TXT).
[RFC5518]	Hoffman, P., Levine, J., and A. Hathcock, "Vouch By Reference," RFC 5518, April 2009 (TXT).
[RFC5617]	Allman, E., Fenton, J., Delany, M., and J. Levine, "DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)," RFC 5617, August 2009 (TXT).

9.2. Informative References

TOC

[RFC4406]	Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail," RFC 4406, April 2006 (TXT).
[RFC4408]	Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1," RFC 4408, April 2006 (TXT).
[RFC4870]	Delany, M., "Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)," RFC 4870, May 2007 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," BCP 26, RFC 5226, May 2008 (TXT).

Author's Address

TOC

	John R. Levine
	Taughannock Networks
	PO Box 727
	Trumansburg, NY 14886
Email:	standards@taugh.com