Network Working Group
Request for Comments: 5518
Category: Standards Track

P. Hoffman
J. Levine
Domain Assurance Council
A. Hathcock
Alt-N Technologies

April 2009

Vouch By Reference

Status of This Memo

Copyright Notice

Abstract

This document describes the Vouch By Reference (VBR) protocol. VBR is a protocol for adding third-party certification to email. It permits independent third parties to certify the owner of a domain name that is associated with received mail.

Table of Contents

1. Introduction

Vouch By Reference, or VBR, is a protocol for adding third-party certification to email. Specifically, VBR permits independent third parties to certify the owner of a domain name that is associated with received mail. VBR may be performed anywhere along the email transit path, by any capable receiving module, either within the handling service or by end-user software.

VBR accomplishes this with a two-part protocol:

- In the first part, a sender affixes VBR information to email messages. The VBR information says which domain certification services the sender believes will vouch for email traffic associated with that sender.

- In the second part, the receiver queries one or more certification services to obtain information about the identity that has been associated with a received message. This latter protocol uses the DNS to distribute the certification information.

A sender provides certification attestations through the use of a new RFC 5322 ([RFC5322]) mail header field, "VBR-Info:". This header field contains the names of services that the sender claims will vouch for it, and the particular type of content of the message. A queried, third-party, DNS-based certification service can respond with a list of the types of message content it will vouch for, such as "transactional mail from somebank.example" and/or "all mail from anotherbank.example".

A prerequisite for successful VBR operation is validation of the identity associated with the message. VBR is based on the use of domain names as identifiers, and permits multiple methods of obtaining and validating domain names. The validation methods are described in the "Obtaining a Useful Domain Name" section below.

The sender performs two steps:

1. Adds a VBR-Info header field to its message

2. Protects the message, as appropriate

If a recipient uses the results of vouching to adjust spam scores on incoming email, that recipient is placing a great deal of operational trust and power in the vouching service. Therefore, recipients need to select such services with care. Further, such recipients may want to select more than one vouching service in order to avoid a single point of failure for setting spam scores.

1.1. Definitions

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].

2. Use of the VBR-Info Header Field

A sender uses VBR to indicate which domain certification services the sender believes will vouch for a particular piece of mail. The certification service uses VBR to state for which signatures it will vouch. This protocol uses the DNS to distribute the certification information.

A message may have multiple VBR-Info header fields. This means that, in the terminology of RFC 5322, VBR-Info is a "trace header field" and SHOULD be added at the top of the header fields.

The content of the VBR-Info header field is a list of three elements:

- The accountable domain
- The type of content in the message
- A list of domain names of services that the sender expects to vouch for that kind of content

The accountable domain is given as md= followed by a domain name. The content type is given as mc= followed by a string; the defined values of that string are found below. The list of services is given as mv= followed by a colon-separated list of domain names.

The formal syntax of the header field is defined in Section 4.

3. Validation Process

A message receiver uses VBR to determine certification status by following these steps:

1. Extracts the domain to certify and the type of message content
2. Verifies legitimate use of that domain using one or more authentication mechanisms as described herein
3. Obtains the name of a vouching service that it trusts, either from among the set supplied by the sender or from a locally defined set of preferred vouching services

4. Queries the vouching service to determine whether the vouching service actually vouches for that type of content for that domain.

4. The VBR-Info Header Field

The VBR-Info header field has the following format:

```
VBR-Info: md=<domain>; mc=<type-string>; mv=<certifier-list>;
```

where <domain> is the domain for which vouching is offered, <type-string> is the content type of the message, and <certifier-list> is a list of domain names of certification providers that the sender asserts will vouch for this particular message. The structure of the <certifier-list> is one or more domain names with a colon (":") between each. The elements in the <domain>, <type-string>, and <certifier-list> must not have any white space in them.

For example, assume that the signer has two companies that are willing to vouch for its transactional notices: certifier-a.example and certifier-b.example. The signer would add the following to the header of its outgoing message.

```
VBR-Info: md=somebank.example; mc=transaction;
    mv=certifier-a.example:certifier-b.example;
```

All three header parameters in the VBR-Info header are mandatory. In particular, there is no default for the md= domain.

Upper and lowercase characters in a VBR-Info header field are equivalent, although conventionally the contents are all in lower case. For upward compatibility, verifiers MUST accept the fields in any order and SHOULD ignore any fields other than the three defined here.

If a message has more than one VBR-Info header field, verifiers SHOULD check each in turn or in parallel until either a satisfactory certifier is found or all the header fields have been checked. All of the VBR-Info header fields in a single message MUST have identical mc= values.

4.1. Syntax of VBR-Info Header Fields

In the ABNF below, the ALPHA and DIGIT tokens are imported from [RFC5234], and the FWS and domain-name tokens are imported from [RFC4871].

```
vbr-info-header =  "VBR-Info:" 1*([FWS] element [FWS] ";")
element = md-element / mc-element / mv-element

md-element = "md=" [FWS] domain-name

mc-element = "mc=" [FWS] type-string
type-string = "all" / "list" / "transaction"

mv-element = "mv=" [FWS] certifier-list
certifier-list = domain-name *(":" domain-name)
```

5. DNS Query

When a recipient wants to check whether a certification claim is valid, it compares the list in the message to the list of services it trusts. For each service that is on the intersection of the two lists, it marshals a domain name to look up that consists of the following DNS labels (from left to right):

- the domain name that asserts it can be certified
- _vouch (a string literal)
- the host name of the vouching service

This domain name is queried for a DNS TXT record. The recipient looks up the domain name in the DNS in the exact same manner it looks up all other domain names.

For example, if a message signed by somebank.example contained the VBR-Info header field above, the receiver might look up either or both of the following names, depending on which vouching service it trusts:

```
somebank.example._vouch.certifier-b.example
somebank.example._vouch.certifier-a.example
```

If the DNS TXT record exists, it contains a space-delimited list of all the types that the service certifies, given as lowercase ASCII. For example, the contents of the TXT record might be:

```
transaction list
```

In the example above, the receiver checks whether or not either certifier vouches for "transaction" mail. That would be indicated by either of the following types: "all" or "transaction" ("all" indicates that the certifier vouches for all message types sent by the domain in question). If either of those types appear in either

TXT record, the certifier has vouched for the validity of the message. Of course, the recipient needs to ignore services that it does not trust; otherwise, a bad actor could just add an authority that it has set up so that it can vouch for itself.

The name for the label _vouch was chosen because any domain name that includes it as one of its labels cannot be a valid host name. There will never be any accidental overlap with a valid host name. Further, it is safe to create a rule that says that a TXT DNS record that comes from a domain name that includes a _vouch label will always have the structure defined in this document.

If the RDATA in the TXT record contains multiple character-strings (as defined in Section 3.3 of [RFC1035]), the code handling that reply from DNS MUST assemble all of these marshaled text blocks into a single one before any syntactical verification takes place.

Verifiers MUST then check that the TXT record consists of strings of lowercase letters separated by spaces, and discard any records not in that format. This defends against misconfigured records and irrelevant records synthesized from DNS wildcards.

The VBR record MUST have only one TXT record.

This query method relies on the considerable advantages of existing DNS efficiencies, reliability, and experience. The lookup is very efficient, and certifiers can add and delete client records as quickly as they want. The lookup also leverages the DNS's negative caching ([RFC2308]).

6. Types of Message Content

This section describes the types of content for which a certifier can vouch. While the rest of the VBR specification is mostly technical and precise, describing the types of contents in mail messages is inherently open to interpretation. Thus, this section makes distinctions as specifically as possible, but the reader needs to understand that these semantic definitions can be interpreted in very different ways by different people.

Note that the value in the mc= element is self-asserted. The purpose of this element is for auditing. There will likely be cases where a certifier will vouch for one type of a sender's mail (such as transactional mail) but not another type (such as advertising). A sender who cannot get anyone to certify its advertising mail, but has a certifier for its transactional mail, might be tempted to cheat and

mislabel it as transactional. The mc= element creates an the audit trail to help their certifiers catch such cheating and allow the removal of the certification for the transactional mail.

Three types of content are defined.

6.1. All

"all" means all mail from the sender.

6.2. List

"list" is the category for email sent to multiple recipients where each piece of mail is identical or is very similar to the others.

6.3. Transaction

"transaction" is the category for transactional messages. This is a response to a specific action of the user, or a notice about an event in the user's account at the sender.

7. Obtaining a Useful Domain Name

VBR relies on having a domain name that specifies a party that is accountable for the message. This requires obtaining the domain name and possessing a strong basis for believing that the use of the domain name is valid, that is, that it has not been spoofed.

There are different ways to achieve this and this section discusses the allowed mechanisms. Senders SHOULD use Domain Keys Identified Mail (DKIM) (and MAY use DomainKeys, Sender Policy Framework (SPF), or SenderID) to give an accountable identity for the sender.

7.1. DKIM

DomainKeys Identified Mail (DKIM), [RFC4871], defines an accountable identity by associating a domain name with the message. It provides assurance that the association is valid through a public-key-based authentication mechanism.

- When DKIM is the validation mechanism, VBR's md= MUST match the domain name taken from one of the DKIM-Signature header fields. If the DKIM signature contains an i= field, the domain name from that field is used; otherwise, the domain name from the DKIM signature d= field is used.

- The VBR-Info header field SHOULD be included in the set of header fields protected by DKIM to prevent a malicious party from changing the contents of the VBR-Info header field or adding bogus VBR-Info header fields.

- The VBR-Info header field SHOULD be added in the header immediately below the corresponding DKIM-Signature header field.

If the DKIM signature validates, the domain name taken from that signature is valid for use with VBR.

7.2. DomainKeys

DomainKeys (DK), [RFC4870], defines an accountable identity by associating a domain name with the message in the d= tag of the DomainKey-Signature header field. It provides assurance that the association is valid through a public-key-based authentication mechanism.

- When DomainKeys is the validation mechanism, VBR's md= MUST be the same value as the domain name found in the DomainKey-Signature d= parameter.

- The VBR-Info header field SHOULD be included in the set of header fields protected by DK to prevent a malicious party from changing the contents of the VBR-Info header field or adding bogus VBR-Info header fields.

- The VBR-Info header field SHOULD be added immediately below the corresponding DomainKey-Signature header field.

If the DomainKeys signature validates, the domain in the d= tag is valid for use with VBR.

7.3. SPF

Sender Policy Framework (SPF), [RFC4408], defines an accountable identity by using an existing message address and querying the DNS to discover whether it is valid for SPF use.

When SPF is the validation mechanism, VBR's md= MUST be the same value as the domain name in the <reverse-path> address that is the first parameter to the SMTP MAIL command.

A domain is valid for use with VBR only when the SPF process produces a "pass" result.

7.4. Sender ID

Sender ID, [RFC4406], defines an accountable identity by using an existing message address known as the Purported Responsible Address ([RFC4407]) and querying the DNS to discover whether it is valid for Sender ID use.

When Sender ID is the validation mechanism, VBR's md= MUST be the same value as the domain name in the Purported Responsible Address in the message.

A domain is valid for use with VBR only when the Sender ID process produces a "pass" result.

8. Security Considerations

VBR is used to allow users to trust independent third parties to certify the owner of a domain name that is associated with received mail. The party validating the mail might use that trust relationship to perform actions that affect the security of their system.

The receiver of a message with a VBR-Info header field MUST ignore certifiers that it does not trust; otherwise, a bad actor could just add an authority that it has set up so that it can vouch for itself.

Implementations SHOULD limit the number of VBR-Info header fields they process in a single message in order to protect themselves from a make-work or denial-of-service attack.

9. IANA Considerations

IANA registered the VBR-Info header field in the Message Header Fields Registry ([RFC3864]) as follows:

Header field name: VBR-Info

Applicable protocol: mail

Status: standard

Author/Change controller: IETF

Specification document(s): RFC 5518

Related information: none

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

10.2. Informative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

[RFC4406] Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", RFC 4406, April 2006.

[RFC4407] Lyon, J., "Purported Responsible Address in E-Mail Messages", RFC 4407, April 2006.

[RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

[RFC4870] Delany, M., "Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)", RFC 4870, May 2007.

[RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

Appendix A. Acknowledgements

Many members of the Domain Assurance Council contributed to the design of the protocol and the wording of this document. In addition, constructive suggestions were received from Jim Fenton and Murray Kucherawy.

Authors' Addresses

Paul Hoffman
Domain Assurance Council

EMail: paul.hoffman@domain-assurance.org

John Levine
Domain Assurance Council

EMail: john.levine@domain-assurance.org

Arvel Hathcock
Alt-N Technologies

EMail: arvel.hathcock@altn.com