MARID
Internet-Draft
Expires: March 16, 2005

M. Lentczner
M. Wong

September 15, 2004

Authorizing Use of Domains in MAIL FROM
draft-ietf-marid-mailfrom-00

Status of this Memo

Copyright Notice

Abstract

Mail on the Internet can be forged in a number of ways. In particular, existing protocols place no restriction in what a sending host can use as the reverse-path of a message. This document describes a protocol whereby a domain can explicitly authorize the hosts that are allowed to use its domain name in a reverse-path, and a way for receiving hosts to check such authorization.

Table of Contents

1. Introduction

The current e-mail infrastructure has the property that any host injecting mail into the mail system can identify itself as any domain name it wants. Hosts can do this at a variety of levels: in particular, the session, the envelope, and the mail headers. While this feature is desirable in some circumstances, it is a major obstacle to reducing end-user unwanted e-mail (or "spam"). Furthermore, many domain name holders are understandably concerned about the ease with which other entities may make use of their domain names, often with intent to impersonate.

This document defines a protocol by which hosts my be authorized by domains to use the domain name in the envelope "Mail From" identity. Compliant domain name holders publish SPF records about which hosts are permitted to use their names, and compliant mail receivers use the published SPF records to test the authorization of hosts using a given "Mail From" identity during a mail transaction.

An additional benefit to mail receivers is that when the use of an identity is verified, then local policy decisions about the mail can be made on the basis of the domain, rather than the host's IP address. This is advantageous because reputation of domain names is likely to be more accurate than reputation of host IP addresses. Furthermore, if a claimed identity fails verification, then local policy can take stronger action against such e-mail, such as rejecting it.

1.1 Terminology

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].

This document is concerned with a portion of a mail message commonly called "envelope sender", "return path", "reverse path", "bounce address", "2821 from", or "mail from". Since these terms are either not well defined, or often used casually, this document defines the "Mail From" identity in Section 2.1. Note that other terms, that may superficially look like the common terms, such as "reverse-path" or "Return-Path" are used only with the defined meanings from normative documents.

2. Operation

2.1 The Mail From Identity

The "Mail From" identity derives from the SMTP MAIL command (see

[RFC2821].) This command supplies the "reverse-path" for a message, which generally consists of the sender mailbox, and is the mailbox to which notification messages are sent if there are problems delivering the message.

This document defines the "Mail From" identity to be mailbox portion of the path of the reverse-path as defined in [RFC2821], Section 4.1.2. when it is non-null.

[RFC2821] allows the reverse-path to be null (see Section 4.5.5.) In this case, there is no explicit sender mailbox, and such a message can be assumed to be a notification message from the mail system itself. When the reverse-path is null, this document defines the "Mail From" identity to be the mailbox composed of the localpart "postmaster" and the domain supplied with the SMTP EHLO or HELO command. Note that requirements for the domain presented in the EHLO and HELO commands are not strict, and software must be prepared for a "Mail From" identity so constructed to be ill formed.

Generally, software that checks the authorization checks described below does so during a SMTP transaction, and so readily has the information required at hand. However, software could perform these checks at a different time, and if so, may extract the reverse-path from the "Return-path" header as described in [RFC2821]. However, it must be noted that while required, not all software complies with inserting such headers. Furthermore, in these cases, if the reverse-path is null, there may not be a reliable way to determine the corresponding EHLO or HELO domain from the "Received:" headers.

2.2 Publishing Authorization

To authorize hosts to use a domain name in the "Mail From" identity, those domains MUST publish SPF records for the domain name as described in [Protocol]. SPF records used for the "Mail From" identity use the "mfrom" scope identifier.

Domains SHOULD publish SPF records that end in "-all", or redirect to other records that do, so that a definitive determination of authorization can be made.

2.3 Checking Authorization

A mail server receiving mail can test the authorization of a client host to inject mail with a given "Mail From" identity. To make the test, the mail receiver MUST evaluate the check_host() function as defined in [Protocol] with the arguments set as follows:

```
<scope>  - the "mfrom" scope identifier
<ip>     - the IP address of the client host that is injecting the
           mail
<domain> - the domain portion of the "Mail From" identity
<sender> - the "Mail From" identity
```

Note that the <domain> argument may not be a well formed domain name. For example, if the reverse-path was null, then the EHLO or HELO domain is used, and that can be an address literal or entirely malformed in a valid SMTP transaction. In these cases, check_host() is defined in [Protocol], Section 3.3, "Initial Processing" to return a Fail result.

Software SHOULD perform this authorization check during the processing of the SMTP transaction that injects the mail. This allows errors to be returned directly to the injecting server by way of SMTP replies. Software can perform the check as early as the MAIL command, though it may be easier to delay the check to some later stage of the transaction.

Software can perform the authorization after the corresponding SMTP transaction has completed. There are two problems with this approach: 1) As described above, it may not be possible to reconstruct the "Mail From" identity. 2) If the authorization fails, then generating a nondelivery notification to the alleged sender is problematic as such an action would go against the explicit wishes of that sender.

2.4 Interpreting the Result

The check_host() function returns one of seven results, some with additional information. This section describes how software that performs the authorization must interpret the results. If the check is being performed during the SMTP mail transaction, it also describes how to respond.

2.4.1 Neutral

A Neutral result MUST be treated exactly like a None result.

2.4.2 Pass

A Pass result means that the client is authorized to inject mail with the given "Mail From" identity. Further policy checks, such as reputation, or black and/or white listing, can now proceed with confidence based on the "Mail From" identity.

2.4.3 Fail

A Fail result is an explicit statement that the client is not authorized to use the domain in the "Mail From" identity. The checking software can choose to mark the mail based on this, or to reject the mail outright.

If the checking software chooses to reject the mail during the SMTP transaction, then it MUST use a 550 reply code with an appropriate message. The Fail result includes a reason. The reason can be used to construct an appropriate message. If the reason is "Not Permitted", then an explanation string is also returned. This explanation string comes from the domain that published the SPF records and may contain a URL. Since that information doesn't originate with the checking software, the checking software will want to make it clear that text is not trusted. Example reply messages for rejecting are:

```
550 SPF Mail From check failed: Malformed Domain

550 SPF Mail From check failed: Domain Does Not Exist

550-SPF Mail From check failed: Not Permitted
550-The domain example.com said:
550 Please see http://www.example.com/mailpolicy.html
```

2.4.4 SoftFail

A SoftFail result should be treated as somewhere between a Fail and a Neutral. This value is used by domains as an intermediate state during roll-out of publishing records. The domain believes the host isn't authorized but isn't willing to make that strong of a statement. Receiving software SHOULD NOT reject the message based on this result, but MAY subject the message to closer scrutiny.

2.4.5 None

A result of None means that no records were published by the domain. The checking software cannot ascertain if the client host is authorized or not.

2.4.6 TempError

A TempError result means that the receiving server encountered a transient error when performing the check. Checking software can choose to accept or temporarily reject the message. If the message is rejected during the SMTP transaction for this reason, the software

MUST use a 450 reply code.

2.4.7 PermError

A PermError result means that the domain's published records couldn't be correctly interpreted for this "Mail From" identity. Checking software SHOULD reject the message. If rejecting during SMTP transaction time, a 550 reply MUST be used.

3. Implications

This section outlines the major implications that adoption of this document will have on various entities involved in Internet e-mail. It is intended to make clear to the reader where this document knowingly affects the operation of such entities. This section is not a "how-to" manual, nor a "best practices" document, and is not a comprehensive list of what such entities should do in light of this document.

This section is non-normative.

3.1 Sending Domains

Domains that wish to be compliant with this specification will need to determine the list hosts that they allow to use their domain name in the "Mail From" identity. It is recognized that forming such a list is not just a simple technical exercise, but involves policy decisions with both technical and administrative considerations.

3.2 Mailing Lists

Mailing lists must be aware of how they re-inject mail that is sent to the list. If the list re-injects mail with the same reverse-path that the mail had when it was received, then that mail may fail the authorization tests defined in this document. In particular, they will fail when the domain of the reverse-path publishes SPF records for the "Mail From" identity, those records do not authorize the mailing list host, and a receiver of the mailing list performs the authorization test.

Almost all mailing list software in use for public mailing lists uses a reverse-path with the mailing list's own domain so that the software can receive mail bounces and assist in the administration of the list. Lists that use such software, configured to operate this way will require only one modest change in light of this document: The mailing list host needs to be authorized by the mailing list domain's own SPF record, if the domain publishes one.

Mailing lists based on simple alias expansion, or other software that doesn't manage bounces directly, may or may not encounter problems depending on how access to the list is restricted. Such lists that are entirely internal to a domain (only people in the domain can send to or receive from the list) are not affected.

3.3 Forwarding Services

Forwarding services take mail that is received at a mailbox and direct it to some external mailbox. At the time of this writing, the near-universal practice of such services is to use the original reverse-path of a message when re-injecting it for delivery to the external mailbox. This means the external mailbox's MTA sees all such mail in a connection from a host of the forwarding service, and so the "Mail From" identity will not in general pass authorization.

There are several possible ways that this authorization failure can be ameliorated. If the owner of the external mailbox wishes to trust the forwarding service, they can direct the external mailbox's MTA to skip such tests when the client host belongs to the forwarding service. Tests against some other identity may also be used to override the test against the "Mail From" identity.

For larger domains, it may not be possible to have a complete or accurate list of forwarding services used by the owners of the domain's mailboxes. In such cases, white lists of generally recognized forwarding services could be employed.

Forwarding services could also skirt the issue by using reverse-paths that contain their own domain. This means that mail bounced from the external mailbox will have to be re-bounced by the forwarding service. Various schemes to do this exist though they vary widely in complexity and resource requirements on the part of the forwarding service.

3.4 Mail Services

Entities that offer mail services to other domains such as sending of bulk mail will may have to alter their mail in light of the authorization check in this document. If the reverse-path used for such e-mail uses the domain of the mail service provider, then the provider needs only to ensure that their sending host is authorized by their own SPF record, if any.

If the reverse-path does not use the mail service provider's domain, then extra care must be taken. The SPF record format has several options for authorizing the sending MTAs of another domain (the service provider's) (see [Protocol].)

3.5 MTA Relays

The authorization check generally precludes the use of arbitrary MTA relays between sender of receiver of an e-mail message. However, the use of open MTA relays on the Internet has long been noted as a security problem. Most sites do not run open relays and many refuse e-mail from known open relays.

Within an organization, MTA relays can be effectively deployed. However, for purposes of this document, such relays are effectively invisible. The "Mail From" identity authorization check is a check between border MTAs.

For mail senders, this means that published SPF records must authorized any MTAs that actually send across the Internet. Usually, this is just the border MTAs as internal MTAs simply forward mail to these MTAs for delivery.

Mail receivers will generally want to perform the authorization check at the border MTAs. This allows mail that fails to be rejected during the SMTP session rather than bounced. Internal MTAs then do not perform the authorization test To perform the authorization test other than at the border, the host that first transferred the message to the organization must be determined, which can be difficult to extract from headers. Testing other than at the border is not recommended.

4. Security Considerations

Most of the security considerations introduced by the authorization check are due to the SPF record format and the operation of the check_host() function. These considerations are described in [Protocol], Section 8, "Security Considerations".

The "Mail From" identity authorization must not be construed to provide more assurance than it does. It is entirely possible for a malicious sender to inject a message with a reverse-path that uses their own domain, to have that domain's SPF record authorize the sending host, and yet the message content can easily claim other identities in the headers. Unless the user, or the MUA takes care to note that the authorized "Mail From" identity does not match the other, more commonly presented identities (such as the From: header), the user may be lulled into a false sense of security.

When the authorization check fails with the code "Not Permitted", an explanation string may be included in the reject response. Both the sender and the rejecting receiver need to be aware that the explanation was determined by the publisher of the SPF record

checked, and is in general not the receiver. The explanation may contain URLs that may be malicious, and/or offensive or misleading text. This is probably less of a concern than it may seem since such messages are returned to the sender, and their source is the SPF record published by the domain in the "Mail From" identity claimed by that very sender. To put it another way, the only people who see malicious explanation strings are people who's messages claim to be from domains that publish such strings in their SPF records.

5. IANA Considerations

None.

6 Normative References

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

[RFC2821] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[Protocol] Wong, M. and M. Lentczner, "The Sender-ID Record: Format and Interpretation", draft-ietf-marid-protocol-03 (work in progress), September 2004.

Authors' Addresses

Mark Lentczner
1209 Villa Street
Mountain View, CA 94041
United States of America

EMail: markl@glyphic.com
URI: http://www.ozonehouse.com/mark/

Meng Weng Wong
Singapore

EMail: mengwong+spf@pobox.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.