individual
Internet-Draft
Expires: October 16, 2006

D. Otis
Trend Micro, NSSG

April 14, 2006

SMTP Name Path Registration
draft-otis-smtp-name-path-00

Status of this Memo

Copyright Notice

Abstract

This document describes a safe means to register delivery paths used by a domain's messages. Message handling might be negatively affected without an apparent relationship between the sending system and the various email related source domains contain within either the message envelope or the message itself. Name based associations can be achieved within a single DNS transaction. The alternative has been to assemble a list of IP addresses for all systems employed to send messages for a domain. The IP address list approach may require hundreds of DNS transactions that endanger the network. The safer name based method accommodates an unlimited number of sending systems, without the overhead and size issues created by a list of IP addresses.

Table of Contents

1. Introduction

Two experimental drafts [I-D.schlitt-spf-classic] and [I-D.lyon-senderid-core] endanger networks by permitting a sizeable exploit devoid of a defensive strategy. See [I-D.otis-spf-dos-exploit]. A safe SMTP name path registration alternative to the SPF script method requires one or two steps. The first step verifies the EHLO of the MTA with a single DNS transaction; see [I-D.crocker-csv-csa]. Once the EHLO is verified, and when the EHLO is within the domain-name in question, no second step is needed. Otherwise, the second step attempts to establish a domain-name association by making a forward reference PTR RRset lookup from the domain in question.

These PTR RRsets would simply list the parent domain of the providers used by the owner of the email-address domain. A dummy domain of "*." would be used to indicate the list represents an open-ended set. An RRset list that only includes a "." label indicates the path list is complete or "closed-ended" and no other domain is associated with the domain. A failure to verify the EHLO or to find an association with the message domain-names may also delay acceptance of the message. The EHLO verification does not create any amplification effects, is comparatively easier to administer, and provides an identifier useful for DoS related protections prior to committing additional resources such as establishing a name path.

2. 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].

Terminology: Terminology conforms to [I-D.crocker-email-arch].

Open-ended: Not all valid elements are included in the set.

Close-ended: All valid elements are included in the set.

3. Name Path Registration

Although many view path registration as a means to reduce spoofing, a reduction only occurs when the relevant email-address domain owner expresses closed-ended paths. Closed-ended paths may cause refusal of messages when the sending system can not be associated with the message source domain-name. Valid messages may be handled by mediators that can not be contained within a path registration. This limitation makes closed-ended paths generally unacceptable, as this

reduces the integrity of email delivery. The primary value of path registration is from the special handling afforded in exceptional cases when no association can be made between a message domain-name and the sending system. This specialized handling may involve the application of white-listing, immediate/delayed acceptance, or ensuring the message is fully vetted prior to acceptance.

Part of the effort of restoring trust in email is adding DKIM [I-D.allman-dkim-base] cryptographic signatures to the messages where the signature verification process itself must be defended. Cryptographic techniques represent a moderate consumption of resources where messages must be fully received before the validity of a signature can be verified. The added overhead makes a cryptographic process more vulnerable to Denial of Service attacks. In addition, any cryptographic scheme is also prone to replay attack.

Defensive schemes MUST be used in conjunction with DKIM and these schemes MUST identify sources based upon either the readily available IP address or verified EHLO to be effective without also endangering the network. Using the IP address may cause collateral blocking when servers are shared, and can not share a common name-based block-list of abusers. Fortunately, SMTP offers a solution for the Denial of Service attack, collateral blocking, the detection of possible message replay, and sharing name-based block-lists. At the beginning of an email exchange session, the host-name of the sending system is provided in the EHLO. EHLO verification MUST become a requisite for immediate message acceptance, and SHOULD BE associated with the signing-domain when the message is signed. Verifying the EHLO permits the same name-based reputations vetting the message sources to also be used in conjunction with name-based reputations defending the cryptographic process.

The following is a table of labels that locate the name path registrations (domain-name lists) for a specific message identity. The domain-names list is returned by the PTR RRsets and represent parent domains of MTAs utilized by the domain found in the message identity. The inclusion of "*." domain indicates an open-ended list of domain-name associations which might modify the handling of messages when a domain association is not discovered. When only a "." domain is returned, this represents a closed-ended list where the identity domain is the only member.

When there are many domain-names being evaluated within a domain, there could be an advantage first requesting the "_oa" PTR domain-name list which might provide an association for other identities. When no association can be discovered for an identity not defined for "_oa" list, a request for the list specifically defined for the identities should be made.

PTR Label	domain-name Reference
_oa._smtp.<domain>	Originating Address
_mf._smtp.<domain>	[RFC2821].MailFrom
_dkim._smtp.<domain>	DKIM signing-domain

"_oa" Identities based on RFC2822 header field domains
Resent-Sender:
Resent-From:
Sender:
From:

Special PTR Domains	Meaning
*.	Part of an open-ended list
.	An empty close-ended list

4. Implementation Examples

The following is an illustrative example for the following received message:

```
EHLO mx-01.example.com
MAIL FROM: <it-dept@example.net>
RCPT TO: <sam@example.org>
DATA
DKIM-Signature: d=example.gov; s=congress;
  a=rsa-sha1; c=simple; q=dns;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00...
To: <staff@example.org>
From: <fred@alumni.example.edu>
...

Don't forget the lunch meeting.
.
QUIT
```

The following EHLO verification and path registration records fully validate this message:

```
     _client._smtp.mx-01.example.com.   IN SRV 1 2 1 mx-01.example.com.

     _oa._smtp.alumni.example.edu.      IN PTR *.

     _oa._smtp.example.biz.             IN PTR .

     _mf._smtp.example.net.             IN PTR example.com.
     _mf._smtp.example.net.             IN PTR *.

     _dkim._smtp.example.gov.           IN PTR example.com.
     _dkim._smtp.example.gov.           IN PTR example.net.
```

This example shows the record used to verify the HELO/EHLO, and the path for message related source domain-names. The path registration for the "_oa" identity at "alumni.example.edu", which includes the [RFC2822].From in the example, indicates this to be an open-ended list. Perhaps no outbound services are provided by the "alumni.example.edu" domain. The path registration for an "_oa" identity at "example.biz" indicates an empty list where no other domain is associated with this domain. The path registration for the "_mf" identity at "example.net" [RFC2821].MailFrom indicates the use of "example.com" services and is marked as being a open-ended list. An open-ended list is indicated by the "*." label which advises that the information is not comprehensive. This example also shows that "example.gov" sends signed messages through MTAs that also EHLO within both the "example.com" and "example.net" domain.

5. IANA Considerations

The label prefixes "_client._smtp.", "_oa._smtp.", "_mf._smtp." and "_dkim._smtp." referencing the different SMTP name path extension will require registration by IANA.

6. Security Considerations

This document describes an option that improves upon the safe use of a path registration mechanism. It is expected that the EHLO verified name is checked against block-lists of reported abusers. When either the EHLO can not be verified, or an association with a message domain can not be established, delayed message acceptance provides another defensive strategy which allows time for abuse to be reported. Delay in acceptance can be accomplished with a Transient Negative Completion, in conjunction with "Requested action aborted: error in processing" SMTP response; see [RFC2821].

7. References

7.1. Normative References

[I-D.crocker-csv-csa]
Crocker, D., "Client SMTP Authorization (CSA)", draft-crocker-csv-csa-00 (work in progress), October 2005.

[I-D.crocker-email-arch]
Crocker, D., "Internet Mail Architecture", draft-crocker-email-arch-04 (work in progress), March 2005.

[I-D.otis-spf-dos-exploit]
Otis, D., "SPF DoS Exploitation", draft-otis-spf-dos-exploit-00 (work in progress), April 2006.

[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.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

7.2. Informative References

[I-D.allman-dkim-base]
Allman, E., "DomainKeys Identified Mail (DKIM)", draft-allman-dkim-base-01 (work in progress), October 2005.

[I-D.lyon-senderid-core]
Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", draft-lyon-senderid-core-01 (work in progress), May 2005.

[I-D.schlitt-spf-classic]
Schlitt, W. and M. Wong, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, version 1", draft-schlitt-spf-classic-02 (work in progress), June 2005.

Author's Address

Douglas Otis
Trend Micro, NSSG
1737 North First Street, Suite 680
San Jose, CA 95112
USA

Phone: +1.408.453.6277
Email: doug_otis@trendmicro.com

Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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