Network Working Group D. Crocker,
Internet Draft Brandenburg InternetWorking
draft−crocker−marid−smtp−validate−00.txt 6 April 2004
Expires: <10−04>

Client SMTP Validation (CSV)

ABSTRACT

Internet mail suffers from the operation of hosts that operate as mail transfer agents (MTA) without any accountability. This makes it impossible to vet MTAs or find recourse when their operation causes problems. The current specification defines a modest mechanism that permits session−time, domain−based validation of peer, client MTAs without prior arrangement between the MTAs. The mechanism is built upon functional components for registering service support and for validating that a name is associated with an IP address. It provides a small, simple and useful improvement to Internet mail service accountability. It is based on well−understood mechanisms and is easily deployed and used. Note that validation does not imply that the MTA is well behaved, merely that it is accountable to the cited domain administrator.

CONTENTS

1. INTRODUCTION

Internet mail suffers from the operation of hosts acting as mail transfer agents (MTA) without any meaningful cross−net accountability. This makes it impossible to vet MTAs or find recourse when their operations cause problems. Many of these hosts have been compromised and turned into unwilling participants in large networks of hostile MTAs that send spam and worms, and contribute to denial of service attacks.

If the client of an exchange can be authenticated, then it is possible to develop an accountability mechanism for it. MUA−MSA exchanges have a substantial number of useful authentication mechanisms available. These are often very strong, and involve significant prior arrangement. The same holds true for MDA−MUA exchanges, and often for MSA−MTA and MTA−MDA exchanges, such as within an organization’s local network.

What is missing is a useful means of authenticating MTA−MTA exchanges over the open Internet. Prior arrangement between such a pair of MTAs is antithetical to the history and operation of Internet mail. Spontaneous communications are at the core of Internet design and operation, as well as at the core of many human interactions. So the challenge is to develop an authentication mechanism that permits the necessary amount of accountability, without imposing undue overhead or restrictions.

The current proposal defines a functional component for determining whether a domain name is authorized to support a service. It defines another functional component for validating that a particular IP Address is associated with a particular domain name. As appropriate, these sub−specifications can be moved to independent documents, to support their use in other services.

The specification combines these components into a mechanism for a session−time, domain−based validation of a peer, client MTA. This is useful across the open Internet, between MTAs that have made no prior arrangement. Validation establishes that the operation of the MTA is accountable to the administrator of the declared domain name.

This proposal is similar to [DRIP], however it built upon different registration and validation mechanisms. It is based on validation of the EHLO domain name and permits detecting machines that are not intended to act as client MTAs but are nonetheless attempting to act as one. The mechanism is designed to be useful between peer MTAs.

It is important to note that validation does not imply that the MTA is well behaved. Policy mechanisms for evaluating the acceptability of an MTA occupy a functional layer above the one that establishes basic authentication. As such, the proposed mechanism merely provides additional information into the pool of considerations for evaluating the client MTA and the message traffic it offers.

Validation of client SMTP agents uses a general, DNS−based validation mechanism. The proposed mechanism is small, simple and useful. It uses well−established mechanisms.

2. TERMINOLOGY

NOTE: This section derives from draft−hutzler−spamops−00.txt. The text has been further elaborated.

The Internet email architecture distinguishes four message−handling components:

- Mail User Agents (MUAs)
- Mail Submission Agents (MSAs)
- Mail Transfer Agents (MTAs)
- Mail Delivery Agents (MDAs)

At the origination end, an MUA works on behalf of end−users to create a message and performs initial "submission" into the transfer infrastructure, via an MSA. An MSA accepts the message submission, performs any necessary pre− processing on the message and relays the message to an MTA for transmission. It implements a server function to the MUA and a client function to the MTA.

MTAs relay messages to other MTAs, in a sequence reaching a destination MDA. Hence an MTA implements both client and server MTA functionality.

The MDA delivers the email to the recipient’s inbox. It implements the MTA server function and the client MDA function. The inbox is part of the recipient−side MUA that works on behalf of the end−user to process received mail.

These architectural components are often compressed, such as having the same software do MSA, MTA and MDA functions. However the requirements for each of these components of the architecture are becoming more extensive, so that their separation is increasingly common.

3. COMPONENT FUNCTIONS

As appropriate, this section may be separated into an independent document.

3.1. DNS−Based Service Authorization Registration (DSAR)

This section defines a generic functional component for registering a domain name to be authorized to support a service.

3.1.1 Authorization Registration Model

This functional component takes a domain name and does a forward query of the [DNS], looking for a specific [SRV] record, to see whether that domain name is authorized to support a particular service. This is a simple registration scheme that validates the name for the service. It does not validate that the name is being used by an authorized party.

3.2.1 Authorization Checking

Authorization registration distinguishes <role>, such as "client" versus "server", and <application>, such as SMTP or LDAP. Use of the DNS authorization component for a specific service requires defining role and application values.

The authorization validation procedure is:

1) Obtain the domain name, <name>. Determining that the name is being used by an authorized party requires separate action.

2) Query the DNS for that domain name, by requesting the _<role>._<application>.name SRV record

3) Evaluate the SRV record, to determine whether the cited domain name is authorized to act as an MTA. (See below for definition of that record.)

If the test is successful, then the client is authorized by the cited domain name to support the cited application service for the specified role.

If there is no SRV record, then there is no statement about authorization.

3.3.1 Service Authorization SRV Record

1) Service

   _<role> is defined by the specific authorization service.

2) Proto

   _<application> is defined by the specific authorization service.

3) Name

   The domain name that is being checked for authorization.

4) TTL

   Standard DNS meaning.

5) Class

   IN

6) Priority

0	=	undefined
1	=	authorized to support the application role
2	=	prohibited from supporting the application role
*	=	other values to be defined

7) Weight

   0

8) Target

   This field MUST be the same as the <name> field.

   There MUST be no more than one _<role>._<application> SRV record for this domain. In effect, this SRV record is used to provide extended registration information about the name, itself, rather than as a means of mapping to other records.

3.4.1 Discussion

This component establishes explicit permission (and accountability) for a particular application service role, associated with a particular domain name. The usefulness of this permission depends upon the ability to validate that the domain name is properly associated with a particular host.

3.2. Host−Name Association Authorization (HNAA)

Is a particular host associated with a particular domain name? Is the host’s use of that domain name −− separate from its performance of any particular service −− authorized?

The typical, underlying means of distinguishing a host on the Internet is through its IP Address (or its set of Addresses.) However, a DNS domain name entry may include reccords that list any IP Address. Even when a domain name is not legitimately associated with a particular host (and it’s IP Addresses), the forward−mapping DNS records for that domain name might list the address. So, the challenge is to determine whether a particular host can legitimately use a particular name. By establishing this relationship, it is then possible to apply policies associated with that name.

3.1.2 IN−Addr.Arpa

The simplest mechanism for determining address−to−name authorization is through the in−addr.arpa branch of the DNS. The security model assumption is that the underlying Internet reliably reports the IP Address of a host. Although this has known limitations, the mechanism is considered sufficient for many, basic uses.

Unfortunately, the in−addr.arpa branch has a long history of being poorly maintained. Hence it might contain the desired information, but it often does not.

QUESTION: Is it safe to nonetheless suggest first looking in in−addr.arpa? Is information there merely incomplete or is it also inaccurate. If the latter, we can’t recommend using it.

If in−addr.arpa can be used to map from the IP Address to the domain name, note that the domain name that is obtained through this mapping must be the same domain name that is registered for the forward, SRV mapping.

3.2.2 Well−Known Domain Names

Assignment of names under a domain name is controlled by the administator of that domain name. It is reasonable to maintain a list of well−known domain names, such as example.com, on the basis of their having accurate and accountable domain name entries. Hence, the service registration entries under their domain names can be interpreted as accurate.

Whether the operational policies of the hosts using those names is acceptable to a particular, remote site, is a separate issue from the accuracy of the information that is listed. Hence a list of such reliable domain names is not a "whitelist" about the site’s policies, but is a whitelist about the accountability of their domain names.

3.3.2 <Phantom third scheme>

<<There is probably another way to validate that a domain name is legitimately associated with a particular host, but I’m not thinking of it, yet. /Dave>>

4. CLIENT SMTP SERVICE VALIDATION

The [MTA] protocol permits an SMTP client to declare its affiliation, by asserting a domain name in the HELO or EHLO (MTA.Helo) announcement. Is this host authorized to act as an SMTP client?

The current proposal takes the domain name asserted by the client MTA and uses the DSAR and HNAA schemes to verify that the use of the name is authorized and that the performance of client SMTP functions is authorized. Establishing whether the host is a well−behaved client SMTP, for example refraining from sending spam, is beyond the scope of this specification.

4.1. Service Validation Mechanism

The procedures for this mechanism are:

1) Validate that use of the domain name is authorized for this host, through the HNAA procedures.

2) Validate that the domain name is authorized to act as a client SMTP, by using the DSAR procedure for the SRV record, as described below.

If these tests are all successful, then the client is authorized by the cited domain name to act as an MTA.

If any of the tests fail, treat the current SMTP session, and associated message traffic, as if no domain name had been asserted in the EHLO announcement.

4.1.1 Client SMTP Registration Record

This section completes the DSAR SRV specification, for registering authorization to act as a client SMTP:

1) Service

   _client

2) Proto

   _smtp

3.2. Discussion

The domain name service is used in different ways and with different schemes for assigning names in the hierarchy. An essential difference in naming is between hosts and services. Naming a host means that the domain name refers only to that one machine. In contrast, naming a service means that the DNS might map the name to multiple machines.

For the mechanisms described in this specification, the domain names MUST be references to individual hosts.

If the mechanism is to be compatible with the

5. MARID WORKING GROUP EVALUATION

This section contains responses to the issues put forward by the MARID working group chairs.

5.1. Amount of change in software components

DNS administration, servers and clients MUST support SRV queries.

Client MTA’s MUST put their registered domain name in EHLO announcements.

Server MTA’s MUST implement the validation procedure described in this specification.

5.2. Configuration complexity

Requires that a validated host have a registered domain name, to list in the MTA.Helo field.

Requires registering each IP Addresses of an authorized client MTA, whenever the set of Addresses changes. No other configuration is required.

5.3. Current use cases that will no longer be viable

All current use cases will still be viable. This mechanism is only enabled by the explicit presence of the defined SRV record for the domain name in the EHLO announcement.

5.4. Needed infrastructure changes

Explicit registration of client MTAs.

5.5. Considerations for use in both IPv4 and IPv6

Validation mechanism is based on IP Addresses and requires the usual query and handling of address types that will be encountered from the IP module and the DNS.

6. SECURITY CONSIDERATIONS

This entire proposal pertains to security, namely authentication and authorization of peer MTAs.

The proposal relies on security of the underlying IP network and on the integrity of DNS data. It performs a basic authentication of the peer MTA, based on domain name registration of the peer’s IP Address. As such, the mechanism provides a basic building block to a larger repertoire of email security services.

A. APPENDIX

A.1. Acknowledgements

Yakov Shafranovich, Marshall Rose, Andrew Newton, John Levine

A.2. References

A.1.2 (Normative)

[DNS] RFC 1035

[MTA] RFC2821, RFC821

[SRV] A. Gulbrandsen, A., P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782; February 2000

A.2.2 Informative

[DRIP] R. S. Brand, L. Sherzer, R. W. Rognlie, "Designated Relays Inquiry Protocol (DRIP)", draft−brand−drip−02.txt

A.3. AuthorsÆ Addresses

Dave Crocker
Brandenburg InternetWorking
675 Spruce Drive
Sunnyvale, CA 94086 USA

Tel: +1.408.246.8253
dcrocker@brandenburg.com

A.4. Full Copyright Statement