marid
Internet-Draft
Expires: August 21, 2005

D. Otis
Mail Abuse Prevention System
D. Crocker
Brandenburg InternetWorking
J. Leslie
JLC.net
February 20, 2005

Client SMTP Authorization (CSA)
draft-ietf-marid-csv-csa-02

Status of this Memo

Copyright Notice

Abstract

Internet operation has typically required no public mechanism for announcing restriction or permission of particular hosts to operate clients or servers for particular services on behalf of particular domains. What is missing is an open, interoperable means by which a

trusted agency can announce authorization for a host to operate a service. The current specification supports this capability for sending SMTP clients. Specifically, is a sending SMTP client permitted to act as a client MTA? Has a separate authority given it permission to perform this service? Client SMTP Authorization (CSA) specifies a DNS-based record that states whether an associated host has permission to operate as a client MTA.

Table of 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. Enhancing the Internet mail transfer service to deal with these issues requires identification, authentication, authorization and accreditation capabilities about the sending SMTP client, as per [ID-CSV]. The current specification addresses the requirement for explicit authorization.

It is important to distinguish this security function from authentication. Authentication establishes that a name is being used legitimately. Authorization establishes that the name is permitted to perform a particular service. The relationship between these two functions is that once a client of an exchange is authenticated, then it is possible to query the permission of that client to perform specific services.

This specification defines a mechanism to permit session-time verification that a connecting SMTP client is authorized to request service as a mail transfer client. The mechanism uses a DNS SRV [RFC2782] record as a basis for verifying that the associated domain name is authorized to act as an SMTP client. The mechanism is small, simple and useful. Separate mechanisms provide the means of authenticating that the domain name is associated with the connecting host, and accrediting the agency that is authorizing the sending host's operation as an SMTP client.

Use of the mechanism specified here MAY also satisfy the authentication requirement. This can occur as a side-effect of the DNS server response optimization that returns IP Address mappings in the Additional Information portion of a response.

Terminology: Terminology conforms to [ID-email-arch].

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].

3. Model

The SMTP [RFC2821], [RFC0821] protocol permits a client to declare its affiliation, by asserting a domain name in the HELO or EHLO announcement.

The current proposal has a receiving SMTP server take the domain name associated with an SMTP client and do a forward query of the DNS. The returned DNS information indicates whether that domain name is authorized by the domain administrator to be an SMTP client.

For efficiency, the DNS response MAY also return authentication information, as per [ID-CSV]. However the authentication functionality is outside the scope of this specification.

4. Mechanism

The receiving SMTP server's authorization procedure is:

1. Obtain a domain name that is associated with the sending SMTP client.

2. Perform a DNS lookup of:
   QNAME = _client._smtp.<name>
   QCLASS = IN
   QTYPE = SRV
   where <name> is associated with the host attempting to obtain service as an SMTP client.

3. If there is no SRV RR matching this QNAME, the CSA information is Unknown; otherwise at least one CSA record exists.

4. If there is a matching QNAME:

   Target addresses MAY be returned in the Additional Data section, or a query for address records of the target name may be needed to determine the associated address(es). This MAY be used to satisfy the authentication function specified in Certified Server Validation [ID-CSV].

   Examine Priority, Weight, and Port, to assess whether the client address is authorized as an SMTP client.

Weight equal to 2 indicates that any client with a valid claim to that EHLO string is authorized to send email. When Weight equals 2, the receiving SMTP server SHOULD check whether the source IP address of the connection is contained in a response (whether returned as Additional Info by the SRV query or returned by a separate address

lookup). If it is not, then the sending SMTP client is NOT authorized when failing the address check.

When Weight equals 1, the sending SMTP client is NOT authorized, regardless of whether its IP address is included in the response.

When Weight equals 3, the sending SMTP client may or may not be authorized, whether or not its IP address is included in the response (but the EHLO name is authorized, if the receiving SMTP server can find some other way to authenticate its right to use that EHLO name).

If the sending SMTP client[ID-CSV] is both authenticated and authorized (with Weight equal 2 and the IP address matching), CSA processing is successful, and the receiving SMTP server can treat messages arriving in this SMTP session as authorized by the EHLO domain administrator.

Otherwise, caution is required. The receiving SMTP server might:

- Generate an SMTP session error, as suggested below.

- Mark the message, to indicate that it failed validation.

- Place the message into a special queue, for separate handling.

For the Unknown case, in which there is no SRV RR, the receiving SMTP server's local policy MAY test whether the domain name, from the HELO/EHLO announcement, is part of a domain that makes an EXPLICIT assertion, as described in Section 5.

When a CSV related session error is generated, a 550 error code SHOULD be used and enough information SHOULD be provided in the reply text to facilitate debugging of the sending system.

5. Client SMTP Authorization SRV Record

The SRV CSA Record has the following contents:

_Service._Proto.Name:TTL:Class:SRV:Priority:Weight:Port:Target

Service:
_client

Protocol:
_smtp

Name:
Domain name asserted in SMTP EHLO announcements.

(These first three fields become the QNAME _client._smtp.Name.)

TTL:
Standard DNS meaning [RFC1035].

Class:
Standard DNS meaning [RFC1035]. SRV-CSA records are only defined for the IN Class.

Priority:
The intended use of [RFC2782] SRV records was to aid discovery and selection of servers by prospective clients. Implementing this client authentication mechanism for the server, the Priority, Weight, and Port fields are no longer used for either discovery or selection. Thus only one SRV-CSA record is needed and these three fields are assigned different meanings. Priority defines the revision level of this mechanism starting at 1.

Weight:
Weight is a group of bit-fields, as follows:

Bit Value	Meaning
1	Ignore Target: The domain name in the Target field is a placeholder, and any IP addresses it resolves to MUST NOT be used for authentication.
2	Authorized: Any host with a valid claim to this name is authorized to send mail.
-	Other bit values are reserved for expansion and must be set to zero.

The resulting unsigned integer values for weight are:

Summed Value	Meaning
0	Should not be used, but MAY be interpreted as the summed value 1.
1	No mail should be coming from clients with this name.
2	Clients with this name are authorized to send mail.
3	Clients with this name are authorized to send mail, but IP addresses associated with the Target field MUST NOT be used for authentication.

Port:

This field allows the domain administrator to declare assertions which apply to all names within the domain, including those names not present in the DNS. At present, only one assertion in the Port field is defined, as follows:

Assertion Bit Value	Meaning
1	Explicit: All authorized names have specific CSV-CSA records.
-	Other bit values are reserved for expansion and must be set to zero. This range of values should be ignored by the recipient when their function is unknown.

Domain administrators MAY assert the "Explicit" bit when they have identified all authorized sending SMTP clients within their domain and published specific CSA SRV records for them; that is, all positive authorizations within the domain are explicitly advertised in DNS.

This enables receiving SMTP servers to reject SMTP sessions with no specific CSV-CSA record if the HELO string is within a domain that asserts explicit authorization.

This assertion greatly simplifies the task of specifying a large class of subdomains which will never legitimately be used as EHLO strings, and makes it practical for large organizations to indicate that individuals should not be using the subdomains assigned to them as EHLO strings. It also deals with invalid EHLO strings that do not appear in the DNS.

Target:
A domain name (typically the same as the EHLO domain) that resolves to the correct list of IP addresses. If this record is defined with the "Ignore Target" bit value, this field should be set to the Name portion of the QNAME, rather than the "." mentioned in [RFC2782], as a means to prevent excessive traffic on root DNS servers by errant implementations.

6. Publishing CSA Records

If a domain administrator declares an assertion about all names within a domain, the appropriate bit MUST be set in the Port field of the CSV-CSA record at the root of the domain for which the assertion applies, and MAY be repeated at subdomains of that domain. The Explicit bit applies to a domain and all its subdomains. If it is repeated in a subdomain it has no effect on the semantics, but it might cause a search to stop sooner.

Domain administrators SHOULD publish records with such assertions in the port field at a level no deeper than sixth-level domains, such as

"_client._smtp.sixth.fifth.fourth.third.second.com"

since receivers are expected to search no deeper than that, and will most likely not find records published for seventh-level or deeper. (Receivers will, of course, still query for the weight field at the exact level of the EHLO string.)

Although a conceptual framework might list the accreditation step as logically following the authorization step, these steps MAY run in parallel. Thus, those responsible for maintaining CSV DNS records should make allowance for the fact that the response of the accreditation service (which depends only on the EHLO string or the client address) is likely to arrive at the receiving MTA before the response to the DNS SRV query detailed here. As a result, the receiving SMTP server may not follow-up partial or truncated UDP responses for expediency. Regardless of what is specified, this receiving SMTP server may decide to refuse the client if their chosen accreditation service returns "Unknown". The following recommendations explain how to ensure that the complete list of IP addresses reaches the receiving SMTP server in the response to its SRV query.

Currently UDP has a limit of 512 octets. Replies requiring more than 512 octets may create UDP fragmentation and, depending upon the connection and handling, in addition to a higher rate of packet loss, may also cause truncated or partial replies. Furthermore, delivery

and resolver handling of truncated and partial responses varies, leading to additional delays and queries. Domain administrators are strongly advised to keep DNS replies below 512 octets for these reasons.

In some cases, domains advertising SRV records will benefit by reassigning some EHLO strings so as to limit the number of IP addresses to be reported in SRV responses. Owing to the efficient nature of the SRV record, the mechanism discussed here calls for a single DNS query per SMTP session (not counting an out-of-band accreditation query), which is substantially less network traffic than per-message methods.

To help ensure complete answers are obtained from cached records, TTL values of the SRV-CSA and related address records should be the same. Beware some DNS server implementations consider the SOA TTL as a default rather than a minimum.

7. Using CSA Records

A receiving SMTP server MAY discover domain assertion information (after finding no record for the specific domain in the EHLO string) by searching for CSV-CSA records in parent nodes of the EHLO string, within the DNS hierarchy. Such a search MUST NOT query a top-level domain (such as COM, NET, or UK), and SHOULD NOT query deeper than a sixth-level domain. Receiving SMTP servers SHOULD ensure that they query a server which caches negative results to avoid useless traffic to the root servers.

Receiving SMTP servers MAY maintain and/or query a database which saves domain-names for which a record has been found with the "Explicit" bit set, and MAY reject or otherwise flag sessions for which the "Explicit" assertion applies but no specific CSV-CSA record is found.

With a complete response to an SRV-CSA query, SMTP server is able to employ Right Hand Side Black List (RHSBL) services based upon the domain name rather than address alone and as well as the accreditation services detailed in [ID-CSVDNA]. These domain-based services will not suffer from the same outdated-record problems as the IP-Address-based services widely used at the time of this writing. Also, of course, domain-based services will be able to accredit those domains which must periodically change their IP address. Reliance on the HELO/EHLO response allows isolation of domains which may share common address space as with virtual hosting or allow detection of domains for which there is insufficient history which may invoke a go-slow approach as example.

8. Security Considerations

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

The proposal also 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.

There is no way a site can keep its hosts from being referenced as servers. This could lead to denial of service.

With SRV, DNS spoofers can supply false addresses. Because this vulnerability exists already with names and addresses, this is not a new vulnerability, merely a slightly extended one. However, as SRV-CSA records are used in an authorization context, the DNS servers can be protected by DNSSEC [RFC3008] should this vulnerability become intractable.

9. IANA Considerations

The tokens "_client" as _Service and "_smtp" as _Proto labels needs to be registered as used with DNS SRV records [RFC2782].

10. Working Group Evaluation

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

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.

2. Configuration complexity
   Requires registering each IP Address of an authorized Client MTA, whenever the set of Addresses changes. No other configuration is required.

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.

4. Needed infrastructure changes
   Explicit registration of Client MTAs.
   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.

11. References

11.1 References - Normative

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC0821] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[RFC1034] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", RFC 1034, November 1987.

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

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

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

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[RFC2782] Gulbrandsen, A., Vixie, P. and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

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

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

[RFC3008] Wellington, B., "Domain Name System Security (DNSSEC) Signing Authority", RFC 3008, November 2000.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

11.2 References - Informative

[ID-CSV] Crocker, D., Otis, D. and J. Leslie, "Certified Server Validation (CSV)", February 2005.

[ID-CSVDNA] Leslie, J., Crocker, D. and D. Otis, "Domain Name Accreditation (DNA)", February 2005.

[ID-email-arch] Crocker, D., "Internet Mail Architecture", July 2004.

Authors' Addresses

Douglas Otis
Mail Abuse Prevention System
1737 North First Street, Suite 680
San Jose, CA 94043
USA

Phone: +1.408.453.6277
EMail: dotis@mail-abuse.org

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

Phone: +1.408.246.8253
EMail: dcrocker@brandenburg.com

John Leslie
JLC.net
10 Souhegan Street
Milford, NH 03055
USA

Phone: +1.603.673.6132
EMail: john@jlc.net

Appendix A. Acknowledgements

John Levine, Tony Finch, and Sam Silberman provided helpful comments.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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