MARID
Internet-Draft
Expires: August 24, 2005

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

Domain Name Accreditation (DNA)
draft-ietf-marid-csv-dna-02

Status of this Memo

Copyright Notice

Abstract

Increased diversity and abuse of access, across the open Internet, mandates additional accountability for sending SMTP clients, in the absence of prior, direct arrangement with receiving SMTP servers.

One means for enabling this is by registration with third-party services that vouch for the policies and accountability of SMTP clients accessing SMTP servers. This specification defines a means for an SMTP client to list third-party services that are prepared to vouch for it, and a means for an SMTP server, or its intermediary, to query vouching services.

Table of Contents

1. Introduction

The Internet mail system, based on SMTP [RFC2821], is designed to allow any client to contact any server. Where prior arrangement is appropriate and may be verified during the session, the client and server can use classic authentication techniques. Increased diversity and abuse of access mandates additional accountability and validation for sessions that do not have the benefit of prior, direct arrangement. One means for enabling this is by having the sending SMTP client registered with a third-party accreditation service that can provide an independent path to information about the policies and performance quality of that client's operator.

This specification defines a mechanism for obtaining such information. It can be operated directly, between the receiving SMTP server and individual direct accreditation services, or it can be used with an indirect/proxy accreditation server working on behalf of the SMTP server, fielding queries to other accreditation services.

The Domain Name Service [RFC1035] provides a common registration environment, so that sending SMTP clients can specify third-party services in which they are listed. The DNS also provides a convenient venue for listing the accreditation information reported by those services.

2. Background

Should a sending SMTP client host (or network) be trusted to be transmit genuine email, rather than problematic messages, such as spam and worms? There are many third-party services that publish their assessments of such hosts and networks. For example, The MAPS-RBL Realtime Blackhole List was established in 1996, listing IP addresses of SMTP clients which sent large amounts of unsolicited email. Another well-known service was ORBS, which listed SMTP clients verified to act as open relays, thereby forwarding mail without any attempt at validation of the sender.

Less well-known are various "whitelist" services, which list SMTP clients assessed to be sending little or no spam. One examples is bondedsender.com; it lists IP addresses of SMTP clients whose owners have posted a bond with bondedsender.com. Each time a recipient of an email passing through one of the bonded SMTP clients complains that the email actually was spam, a portion of that bond is forfeit to a non-profit organization. Another example is Habeas.com, authorizing senders to include a copyrighted text string, to show certification.

3. Accreditation Services

Third-party services can list sending SMTP clients that guard against sending unsolicited bulk email or they can list those that are known to be a problem. This provides a mechanism for establishing trust between clients and servers that have had no prior contact. This specification does not deal with the internal operation of such third-party services.

Accreditation services must, themselves, be assessed for the criteria they use. Some will have trivial criteria, offering no serious quality assurance. Others will be so strict as to have very narrow utility. Still others may use criteria that go wildly astray from a sender's care in obtaining and using recipient addresses. For example the accreditation service might base their assessment on the listee's political views. Hence it is the responsibility of the host querying the accreditation service to evaluate the operation of the accreditation service, itself, and treat the weightings they offer accordingly.

Finding Appropriate Accreditation Services: With millions of domains and hundreds of expected accreditation services, a core challenge is to find the particular direct accreditation services that evaluate a particular sending SMTP client. For that reason, sending SMTP clients SHOULD advertise lists in which they appear. This is intended as a convenience for receiving SMTP servers, and those servers MAY consult any accreditation services they wish.

A sending SMTP client SHOULD register accreditation services in which it is listed by including DNS records with domain-names of the accreditation services. The client SHOULD place such records at each sub-domain level that receiving SMTP servers will need to validate. In cases where the domain management wishes to advertise the same list for any subdomain name, wildcard DNS records MAY be used.

(Note that the existence of these DNS records does not certify that a sending SMTP client has a valid claim to the name it places in the EHLO command; this requires a separate mechanism, to ensure that the client is authorized to use that name.

Clients SHOULD list more than one accreditation service, so that it is likely at least one service will be acceptable to a receiving SMTP server that is making the query. Indeed, it is likely that some direct accreditation services will develop a reputation for being "spam-friendly" and be considered worthless for reputation purposes. In other cases, the receiving SMTP server or its proxy may have no way to rate a particular direct

accreditation service the sending SMTP client uses, and it will be ignored.

In order to facilitate resolution of problematic listings, a receiving SMTP server that refuses access to a sending SMTP client, due to an unfavorable recommendation, SHOULD return an error message that cites the accreditation service(s) providing the basis for the rejection.

4. Listing Pointer Service Record Template

A domain may list services that provide accreditation information about the operations associated with that name. The DNS records they SHOULD list are in the form:

1. Name: The domain name that will be checked

2. Type: PTR

3. Class: IN

4. TTL: Standard DNS meaning

5. Target: QNAME string (starting with "_VOUCH._SMTP.") for a DNS SRV query to return the preferred access method for human-readable queries to a suggested accreditation service.

Concatenating (with a single dot between them) the domain name of a sender recommending this service with this target domain name (without the "_VOUCH._SMTP.") and doing a DNS query for a TXT record SHOULD return a string giving a report on the trustworthiness of the client domain.

5. Accreditation Procedure

A receiving SMTP server MAY validate a sending SMTP client by:

1. Obtaining the domain name of the client.

2. Determining that the name is being used by an authorized party.

3. Creating a list of accreditation services to query, both those the client has registered and those obtained by the server through other means -- such as those that perform block-listing -- to query.

4. Querying those services for assessments of the host associated with that name.

5. Synthesize a single assessment using the responses from the multiple services; this is done according to whatever weightings and other methods local policy may dictate.

6. Returning the recommendation -- with a value of "unknown" if no records were found or if none of the recommended accreditation services are known.

Alternatively, the receiving SMTP server MAY query any trusted accreditation service which itself performs steps 3 through 6 and reports a single recommendation.

In the event that the query procedure is unable to produce a useful assessment, the decision on how much trust to place in the client is outside the scope of this document.

If the final report is "not recommended", the server SHOULD return an error including the name of an accreditation service that reported Not-Recommended. We suggest using "550 Access Denied based on <accreditation-service-domain-name> report."

6. Accreditation Report Record Template

A direct accreditation service MUST publish its listings using the following record and format:

1. Name: <domain being checked>.<Accreditation Service>.

2. Type: TXT

3. Class: IN

4. TTL: Standard DNS meaning

5. Target: Accreditation Report string.

The Accreditation Report string MUST contain a report for a particular service, encoded as:

1. service accredited

2. comma

3. level accredited for (service-specific, may be empty)

4. comma

5. recommendation, specified as:

1. 'A' for Strongly Recommended

2. 'B' for Recommended

3. 'C' for Unknown

4. 'D' for Not Recommended

5. 'E' for Strongly Not Recommended

6. semicolon (or end-of-string)

7. optional info (format is local to each accreditation service).

Strings which do not match this format MAY have meaning outside the scope of this specification and MUST be ignored by DNA parsers unaware of such meaning.

For MARID-CSV, the "service accredited" MUST be "MARID" and the "level accredited" currently MUST be "1".

The "Accreditation Service" string portion of the Query Name above should match the RDATA string of the Suggested Service Record published by the domain being checked, with the "_VOUCH._SMTP." substring removed.

7. Discussion of DNS record types

For the DNS records listing recommended accreditation services, we have chosen to use the existing PTR record type. It is perfectly suited to our needs, yielding a domain-name as the answer and having no known competing uses at the subdomain levels matching likely EHLO strings. Conflicts with possible future uses are prevented by prefixing the substring "_VOUCH._SMTP." so as to point to a SRV query string. Any CSV queries MUST discard any PTR records returned which do not contain that prefix.

For the DNS records giving accreditation reports, we have chosen the existing TXT records. We believe that accreditation services should be given the full flexibility of free-format text in addition to the limited formatted text we specify here. There should be no future conflicts except for accreditation relating to other services, for which we specify that each TXT record should start with the name of the service being accredited. Since all these records are at subdomains generated by concatenating two different domain names, naming conflicts for the query string cannot arise unless the accreditation service chooses subdomain (host) names which overlap top-level domain names.

For both record types, wildcards will work. Domain management can specify the same accreditation service(s) for all possible subdomains with wildcard PTR record(s). Accreditation services can specify the same accreditation report for all possible subdomains with a single TXT record.

8. Security Considerations

This entire proposal pertains to security, namely authorization and verification of clients seeking services.

It specifies a way for client domains to advertise the names of accreditation services in DNS. Various well-known attacks on DNS services may result in failure to respond to queries or in the receipt of out-of-date information. However, servers need not use this information directly, and are more likely to use out-of-band methods to query their preferred accreditation service.

9. References - Normative

[ID-Marid-CSV] Crocker, D., Otis, D. and J. Leslie, "Certified Server Validation (CSV))", July 2004.

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

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

Authors' Addresses

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

Phone: +1.603.673.6132
Email: john@jlc.net

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

Phone: +1.408.246.8253
Email: dcrocker@brandenburg.com

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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