Network Working Group R. S. Brand
Internet-Draft L. Sherzer
Expires: December 23, 2003 June 24, 2003

Designated Relays Inquiry Protocol (DRIP)
draft-brand-drip-00.txt

Status of this Memo

Copyright Notice

Abstract

The Designated Relays Inquiry Protocol, DRIP, is a method for domain name owners to specify the IP addresses that are authorized to relay mail as a domain name. The protocol provides a method for server MTAs to reject SMTP connections from IP addresses not authorized to use a domain name.

Table of Contents

1. Introduction

The Designated Relays Inquiry Protocol, DRIP, is a method for domain name owners to specify the IP addresses that are authorized to relay mail as a domain name in the SMTP HELO and EHLO commands. The protocol provides a method for server MTAs to reject SMTP connections from IP addresses not authorized to use the domain name given in the SMTP HELO and EHLO commands.

1.1 Motivation

Source verification information transmitted as part of a mail message, such as digital signatures, can permit MTAs, MDAs, and MUAs to verify that a messages is associated with a sender or gateway. However, those methods do not prevent malware authors from:

- Embedding a verifiable (signed) message in the malware.
- Embedding a verifier generator (private key) in the malware.

Either technique permits malware afflicted machines to send verifiable messages.

DRIP is designed to force malware authors to send the malware generated mail through the relays the afflicted systems are already configured and authorized use. Operators of those relays are very likely to have an existing relationship with the operators of the afflicted systems and can act to limit the damage to the internet caused by the malware.

1.2 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].

DNS
: Domain Name System. See [RFC1034] and [RFC1035].

IPv4
: Internet Protocol version 4.

IPv6
: Internet Protocol version 6.

ISP
: Internet Service Provider.

Malware
: Malicious software. See [RFC2828].

MDA
: Mail Delivery Agent.

Mail Relay
: See MTA.

MTA
: Mail Transfer Agent.

MUA
: Mail User Agent.

Relay
: See MTA.

SMTP
: Simple Mail Transfer Protocol. See [RFC2821]

Standardese
: A peculiar dialect employed by authors of standards.

2. Overview

Domain name owners identify and record the IP addresses that are authorized to relay mail as their domain name. How the IP addresses are identified is beyond the scope of this document, but will likely involve consultation with the postmaster for the domain name. The IP address authorization records are recorded in DNS as described in Section 3.

Server MTAs verify the domain name the client MTA submitted as identification, by querying for the IP address authorization records recorded by the domain name owner. Based on the result of the query, the server MTA can determine if the domain name is a DRIP participant. If the domain name is a DRIP participant, the result of the query will also indicate if the IP address of the client is authorized to use the domain name to relay mail. Section 4 specifies the operation of server MTAs following this protocol.

3. Designating Relays

Domain name owners record the designated relays by adding a specifically formatted DNS record for each IP address that is authorized to use a domain name in the SMTP HELO or EHLO commands. Default records are also added to indicate DRIP participation by the domain name, and that the IP address used in the query is NOT authorized to use the domain name to relay mail.

3.1 Designation Record Template

The template for the DNS records is:

```
${IPS}.${IPV}.relays._email_.${DOMAIN}.   IN   ${TYPE}   ${IP}
```

With:

${IPS}
: The textual representation of the IP address.

${IPV}
: The textual representation of the IP protocol version used.

${DOMAIN}
: The domain name used in the SMTP HELO or EHLO commands.

${TYPE}
: The DNS record type corresponding to the IP protocol version of the IP address.

${IP}
: The IP address.

See [RFC2782] for a discussion of the need for the underscores.

3.2 Default Designation Records

The following default or "wildcard" records are added for each domain name and defined IP protocol version. These records, when returned as a result of a DRIP query, indicate DRIP participation by the domain name and that IP address used in the query is NOT authorized to use the domain name in the SMTP HELO or EHLO commands.

```
*.${IPV}.relays._email_.${DOMAIN}.   IN   ${TYPE}   ${IPZ}
```

Where ${IPZ} depends on the IP protocol version.

A default record returned as the result of a DRIP query is identified by the value of the record, ${IPZ}, which is defined for each IP protocol version and corresponds to the "unspecified address".

Both IPv4 and IPv6 default designation records SHOULD be added for each domain name.

3.3 IPv4 Designation Records

For IP version 4 addresses, the following applies:

${IPS}
: Textual representation of the IPv4 address of the Designated Relay in "dotted quad", also known as "dotted decimal", notation. This textual representation was chosen to be easy for both the wetware components and the software components to implement the protocol.

  The textual representation of the IPv4 loopback address, 127.0.0.1, is

  ```
  127.0.0.1
  ```

${IPV}
: "IPv4".

${TYPE}
: "A".

${IP}
: The IP address of the the Designated Relay.

${IPZ}
: "0.0.0.0", the IPv4 "unspecified address". Chosen because it can not be a valid client IP address when used with TCP.

3.4 IPv6 Designation Records

For IP version 6 addresses, the following applies:

${IPS}
Textual representation of the IPv6 address of the Designated Relay formatted as a sequence of 8 16bit words separated by dots. Each word is represented by 4 hexadecimal digits. The words and the hexadecimal digits of a word are in network byte order. This IPv6 address representation is similar to the representation in [RFC3513] except that the colons have been replaced with dots, and that leading zeros MUST be included. This textual representation was chosen to be easy for both the wetware components and the software components to implement the protocol.

The textual representation of the IPv6 loopback address, ::1, is:

0000.0000.0000.0000.0000.0000.0000.0001

The textual representation of the IPv6 address 2002:c000:201::1234 is:

2002.c000.0201.0000.0000.0000.0000.1234

${IPV}
"IPv6".

${TYPE}
"AAAA".

${IP}
The IP address of the the Designated Relay.

${IPZ}
"::", the IPv6 "unspecified address". Chosen because it can not be a valid client IP address when used with TCP.

MTAs with IPv4-compatible IPv6 addresses [RFC3513] SHOULD also have an IPv4 DRIP record for the IPv4 part of each IPv4-compatible IPv6 address.

3.5 Designation Examples

3.5.1 Designation Example 1

The owner of the domain name EXAMPLE.COM would add the following DNS records to the EXAMPLE.COM zone to indicate that the domain name EXAMPLE.COM is NOT valid for use in the SMTP HELO and EHLO commands.

Default Designation Records:

```
*.IPv4.relays._email_.EXAMPLE.COM.     IN    A      0.0.0.0

*.IPv6.relays._email_.EXAMPLE.COM.     IN    AAAA   ::
```

IPv4 Designation Records:

None.

IPv6 Designation Records:

None.

3.5.2 Designation Example 2

The owner of the domain name M.EXAMPLE.COM would add the following DNS records to the M.EXAMPLE.COM zone to indicate that ONLY the IPv4 addresses 192.0.2.10, 192.0.2.11, and 127.0.0.1 are authorized to use the domain name in the SMTP HELO and EHLO commands.

Default Designation Records:

```
*.IPv4.relays._email_.M.EXAMPLE.COM.    IN    A      0.0.0.0

*.IPv6.relays._email_.M.EXAMPLE.COM.    IN    AAAA   ::
```

IPv4 Designation Records:

```
192.0.2.10.IPv4.relays._email_.M.EXAMPLE.COM.  IN A  192.0.2.10

192.0.2.11.IPv4.relays._email_.M.EXAMPLE.COM.  IN A  192.0.2.11

127.0.0.1.IPv4.relays._email_.M.EXAMPLE.COM.   IN A  127.0.0.1
```

IPv6 Designation Records:

None.

4. MTA Operation

Server MTAs use the IP address of the client MTA from the SMTP connection and the domain name, which the client submitted as identification in the SMTP HELO or EHLO command, to verify that the IP address is authorized to use the domain name to relay mail. The process for doing this is:

1. Attempt to retrieve the DRIP authorization record for the IP address and the domain name via DNS.

2. Examine the result of the DNS retrieval attempt to determine the DRIP status.

3. Continue or terminate the SMTP transaction based on the DRIP status.

DRIP authorization checks may be deferred until the MAIL command in the SMTP transaction or not be performed at all for SMTP transactions where relay authorization schemes are used. Examples of relay authorization schemes are, an ISP's use of the client's IP address to allow only the ISP's customers to relay; or a corporate server MTA using SMTP AUTH to allow roaming senders to relay.

4.1 DRIP Authorization Retrieval

The DRIP authorization record to retrieve is the DNS record, as described in Section 3.1, corresponding to the IP address and domain name that the client MTA identified itself as.

IPv6 server MTAs MUST perform the DRIP authorization retrieval using the IPv4 address of the "IPv4-mapped IPv6 address" [RFC3513] when clients connect from IPv4-mapped IPv6 addresses.

4.2 DRIP Status Determination

A successful retrieval of a single record of the appropriate type with the IP address in the record matching the IP address of the client has a DRIP status of DRIP_OK. The requirement that the IP address in the authorization record be the IP address of the client, is to prevent malware authors from easily designating the entire IP address space as authorized to relay as a given domain name.

A successful retrieval of a single record of the appropriate type with the IP address in the record not matching the IP address of the client has a DRIP status of DRIP_NOT_OK.

Any type of temporary DNS retrieval or network failure has a DRIP status of DRIP_TEMP_FAIL.

Any other type of DNS result, such as a permanent error, multiple records retrieved, retrieved record not of the correct record type, etc., has a DRIP status of DRIP_UNKNOWN.

4.3 DRIP Status Meanings

The DRIP statuses have the following meanings:

DRIP_OK
: This indicates that the IP address of the client is one of the authorized IP addresses for the domain name to use to relay mail. The SMTP transaction may continue.

DRIP_NOT_OK
: This indicates that the IP address of the client is not one of the authorized IP addresses for the given domain name to use to relay mail. The SMTP transaction SHOULD be terminated with a permanent failure, 5XX, reply code.

DRIP_TEMP_FAIL
: This indicates that the lookup could not be completed at this time. The SMTP transaction SHOULD be terminated with a temporary failure, 4XX, reply code.

DRIP_UNKNOWN
: This indicates that the given domain name is not a DRIP participant. Local policy of the server MTA determines if the SMTP transaction should continue or not.

  A RECOMMENDED local policy is for the server MTA to, iteratively, use the parent domain names to perform more DRIP authorization retrievals. If any of those retrievals result in either a DRIP_OK status or a DRIP_NOT_OK status, the server MTA SHOULD assume that the client is NOT authorized to relay mail as the given domain name.

4.4 MTA Operation Examples

The following examples assume that the DNS records described in Section 3.5 exist and that no other DRIP related DNS records exist for the domain names used.

4.4.1 MTA Operation Example 1

A server MTA accepts an SMTP connection from IP address 192.0.2.10 and the client identifies itself as M.EXAMPLE.COM.

1. The server attempts to retrieve the DRIP authorization record

   192.0.2.10.IPv4.relays._email_.M.EXAMPLE.COM. IN A 192.0.2.10

   via a DNS lookup.

2. The DNS lookup retrieves a single A record with the IP address 192.0.2.10.

3. Since only a single record was retrieved, it was of the correct type, and IP address in the record is the IP address of the client, the DRIP status is DRIP_OK.

4. The SMTP transaction continues.

4.4.2 MTA Operation Example 2

A server MTA accepts an SMTP connection from IP address 192.0.2.99 and the client identifies itself as S.EXAMPLE.COM.

1. The server attempts to retrieve the DRIP authorization record

   192.0.2.99.IPv4.relays._email_.S.EXAMPLE.COM. IN A 192.0.2.99

   via a DNS lookup.

2. The DNS lookup results in a "Name Error", indicating that the record does not exist.

3. Since the DNS lookup resulted in a permanent lookup error, the the DRIP status is DRIP_UNKNOWN and the server uses local policy to determine if the SMTP transaction should continue or not.

4. If the server follows the RECOMMENDED local policy of performing DRIP authorization retrievals using parent domain names when a DRIP status of DRIP_UNKNOWN is encountered, the server attempts to retrieve the DRIP authorization record

   192.0.2.99.IPv4.relays._email_.EXAMPLE.COM. IN A 192.0.2.99

   via a DNS lookup.

5. The DNS lookup retrieves a single A record with the IP address 0.0.0.0.

6. Since only a single record was retrieved, and the record was of the correct type, and the IP address in the record is not the IP address of the client, the DRIP status is DRIP_NOT_OK.

7. Because this was a DRIP authorization retrieval of a parent domain and the status is of this retrieval is DRIP_OK or DRIP_NOT_OK, the server SHOULD assume that the client is NOT authorized to relay mail as the given domain name.

8. The server terminates the SMTP transaction with a permanent failure, 5XX, reply code.

4.4.3 MTA Operation Example 3

A server MTA accepts an SMTP connection from IP address ::FFFF:C000:263 and the client identifies itself as S.EXAMPLE.COM.

Because the IP address of the client is the IPv4-mapped IPv6 address of 192.0.2.99, the server MUST perform the same operations as in Section 4.4.2.

5. Security Considerations

This method relies on DNS to verify relay authorization and as such is vulnerable to the security issues of DNS. However, this is no different than mail, in general, being vulnerable to DNS security issues. Sites concerned about this should investigate implementing [RFC2401] and/or [RFC2535].

A likely, and intended, response of malware authors to wide spread adoption of DRIP is to search afflicted systems for MUA settings and use the configured gateways, and possibly identities and credentials, to mail their payloads. It is hoped that the gateway operators will notice the undesirable traffic and be able to do something about it. The gateway operators already have a relationship with the operator(s) of the afflicted systems and are in a much better position, than the internet at large, to be able to correct the problem.

DRIP is intended and designed to help protect your systems from the malware afflicted systems of others. Not to protect your systems from your own malware afflicted systems. Sites concerned about this should investigate the use of malware detectors on their systems.

While not a security consideration, DRIP does not provide any assurances to the server MTA that the mail being relayed from the client is not SPAM; only that the IP address of the client MTA is authorized to relay mail as the domain name, the client identified itself as, in the SMTP EHLO or HELO command.

Normative References

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

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

[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.

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

Informative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1886] Thomson, S. and C. Huitema, "DNS Extensions to support IP version 6", RFC 1886, December 1995.

[RFC1925] Callon, R., "The Twelve Networking Truths", RFC 1925, April 1996.

[RFC1983] Malkin, G., "Internet Users' Glossary", RFC 1983, August 1996.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

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

[RFC2828] Shirey, R., "Internet Security Glossary", RFC 2828, May 2000.

Authors' Addresses

Raymond S Brand
P.O. Box 100486
Ft. Lauderdale, FL 33310
US

EMail: rsbx@acm.org
URI: http://www.RSBX.com/

Laurence Sherzer
P.O. Box 5072
Deerfield Beach, FL 33442
US

EMail: laurence@sherzer.net
URI: http://www.sherzer.net/

Appendix A. Dictatorial Powers

Any measure to control SPAM, if it is to be effective, must create or enhance the power of one or more entities involved in moving email from the source to the destination(s).

The method described in this document enhances the ability of the domain name owner to control which MTAs may identify themselves as a domain name.

Appendix B. Acknowledgments

The authors gratefully acknowledges the contributions of: Robert M. Bownes III, and Richard Rognlie.

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

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