Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: March 30, 2012

M. Parthasarathy, Ed.
Apple Inc.
P. Vixie
ISC

September 27, 2011

draft-mohan-dns-query-xml-00

Abstract

This memo presents a technique for representing DNS messages using XML. This enables DNS query transactions to be transported over HTTP/HTTPS.

Status of this Memo

This Internet-Draft will expire on March 30, 2012.

Copyright Notice

Table of Contents

1. Introduction

Domain Name System (DNS) is specified in RFC 1035 [RFC1035] and its security extensions (DNSSEC) are specified in RFC 4034 [RFC4034] and RFC 4035 [RFC4035]. DNSSEC provides origin authentication and integrity protection for DNS data. While signing the authority data and verifying such signatures in recursive or stub validators are well understood and well solved problems, the channel between authority servers and validators is commonly unusable for DNSSEC-secured transactions due to overreach in customer premises equipment, firewalls, intrusion detection systems, and non-DNSSEC-aware recursive name servers operated by enterprises or service providers. HTTP [RFC2616] is known to work in such environments and has become the de facto tunneling protocol in the Internet. To facilitate tunneling DNS messages over HTTP, this document describes a method of encoding a DNS message, including the resource records, as an XML object [XML].

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Protocol Overview

In traditional DNS communication, the DNS stub resolver communicates with a recursive server which in turn communicates with the authoritative servers to fetch the DNS data. To fetch the DNS XML data, the resolver communicates with a web server using HTTP/HTTPS. It issues a GET request with parameters using the URI format in [RFC2396] indicating the attributes of the query as it would do in a normal DNS query. The web server on receiving the request retrieves the DNS data and formats in XML before sending it back to the resolver. The resolver may issue multiple DNS queries either using a single or multiple TCP connection to the server whose details are beyond the scope of this document.

3. DNS XML Query

The resolver issues a HTTP GET request with parameters to fetch the DNS XML data. The structure of the query is as follows:

```
https://server_address/dns_service/
query?name=NAME&type=TYPE&ID=VALUE&RD=VALUE&CD=VALUE&DO=VALUE
```

dns_service - tells the web server that the GET request is to fetch the DNS records

query - indicates that this GET request is a DNS query and it should return the DNS Response formatted in XML

name - The domain name being looked up

type - Type of the query as specified under "TYPE" field in the RRTYPE registry in [IANA_DNS].

ID - Corresponds to the ID value in the DNS query. When there are multiple queries in flight, the ID in the response can be used to match the request.

RD - Corresponds to the "RD" bit in the DNS query. Set to 1 if recursion is desired or 0 otherwise.

CD - Corresponds to the "CD" bit in the DNS query. Set to 1 if validation will be done by the end host or 0 otherwise.

DO - Corresponds to the "DNSSEC OK" bit in the DNS query. It reflects the setting of the DNSSEC OK bit in EDNS0 option.

4. XML Representation of DNS Message

The XML representation of the DNS message maps the DNS header specified in section 4.1.1 of [RFC1035] to XML representation.

5. DNS Message Format

The DNS message is enclosed under the root element "response", under which all the other elements appear.

```
<response>

      All the other elements are enclosed within this element.

</response>
```

The XML representation of the DNS header does not represent all the fields. Only RCODE, the AA bit and the CD bit of the second sixteen bit field (that follows the ID field) is represented. The fields

QDCOUNT and the question section are omitted. If the resolver converts the XML representation into binary format for processing, the omitted fields should be inferred appropriately. Rest of the fields are described below.

<id>

The value of this field is copied from the HTTP request parameters. It is used by the resolver to match the response to the request.

</id>

<aa>

Corresponds to the AA bit in the header. If AA is set, this element is set to 1 and otherwise 0.

</aa>

<ad>

Corresponds to the AD bit in the header. If AD is set, this element is set to 1 and otherwise 0.

</ad>

<cd>

Corresponds to the CD bit in the header. If CD is set, this element is set to 1 and otherwise 0.

</cd>

<rcode>

RCODE of the response represented as specified under "Name" field of the RCODE registry in [IANA_DNS].

</rcode>

<anscount>

Number of answers in the answers element described below

</anscount>

<answers>

This section contains all the records in the answer section of the response with each resource record in the answer element.

<answer>

Each answer element contains a resource record

</answer>

</answers>

<nscount>

Number of authorities in the authorities element described below

</nscount>

<authorities>

This section contains all the records in the authority section of the response with each resource record in the authority element.

<authority>

Each authority element contains a resource record

</authority>

</authorities>

<arcount>

Number of additional records in the additionals element given below

</arcount>

<additionals>

This section contains all the records in the additional section of the response with each resource record in the additional element.

<additional>

Each additional element contains a resource record

</additional>

</additionals>

6. DNS Resource Record Format

Every DNS resource record contains a name, type, class, ttl, rdlength and type specific rdata. The XML elements for each of these are described below.

<name>

Textual representation of the domain name to which this resource record pertains as it appears in the master file

</name>

<type>

Type of the RDATA field as specified under "TYPE" field in the RRTYPE registry in [IANA_DNS].

</type>

<class>

Class of the RDATA field as specified under "Name" field in the Class registry in [IANA_DNS].

</class>

<ttl>

Time to live value of this resource record in seconds

</ttl>

<rdlength>

Length of the RDATA field

</rdlength>

<rdata>

RDATA is represented as zero or more words of hexadecimal data described in RFC 3597 [RFC3597]. The special token \# and RDATA length are not included.

</rdata>

7. Message Compression

Message compression is not supported. All names should be fully expanded.

8. Message Update

DNS Update RFC 2136 [RFC2136] is not supported.

9. Acknowledgements

TBD

10. IANA Considerations

This memo includes no request to IANA.

11. Security Considerations

In the current DNS system, there is no trust relationship between the stub resolver and the rest of the system. When the users connect to the Internet using their ISP that provides the Internet service, they expect the ISP to provide trustworthy DNS service. When they connect to the Internet from hotspots and other places, there is no trust whatsoever. There are also many popular open recursive resolvers that are available in the Internet today that provide DNS resolution. Similarly, the DNS service described in this document may be provided via both HTTP and HTTPS. Depending on the stub resolver's trust relationship with the DNS service provider, it can use HTTP or HTTPS. When DNSSEC is used, the DNS data can be authenticated independently.

DNSSEC itself cannot be used to validate the IP address of the server that is providing the DNS service using the method described in this document.

12. References

12.1. 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.

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, September 2003.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

12.2. Informative References

[IANA_DNS] "Domain Name System Parameters", <http://www.iana.org/assignments/dns-parameters>.

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[XML] T, Bray., J, Paoli., and Sperberg-McQueen. C.M., "Extensible Markup Language (XML)", 1998.

Appendix A. Appendix A

This section provides a few sample queries and responses

```
QUERY: https://server_address/dns_service/
query?name=www.isc.org&type=A&ID=2345&RD=1

RESPONSE:

<?xml version="1.0" encoding="US-ASCII"?>

<response>

   <ID>2345</id>

   <aa>1</aa>

   <rcode>0</rcode>

   <anscount>1</anscount>

   <answers>

      <answer>9514402A</answer>

   </answers>

</response>
```

Authors' Addresses

Mohan Parthasarathy (editor)
Apple Inc.
1 Infinite loop
Cupertino, 95014
USA

Phone: +1 408 862 7901
Email: mparthasarathy@apple.com

Paul Vixie
ISC
950 Charter Street
Redwood City, 94063
USA

Phone: +1 650 423 1300
Email: vixie@isc.org