Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 30, 2012

W. Kumari
Google
R. Arends
Nominet
February 27, 2012

EDNS Echo.
draft-wkumari-dnsext-echo-00

Abstract

This document describes a DNS protocol extension to allow for arbritry data to be inserted into a DNS Request and have that same data be returned in a DNS Reply.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

Table of Contents

1. Introduction

RFC2671 [RFC2671] specifies an extension mechanism for DNS. This document describes an EDNS option to allow for arbritry data to be inserted into a DNS Request and have that same data be returned in a DNS Reply. This functionality can be used to increase the effective size of the ID field [RFC1035, Section 4.1.1 [RFC1035]] and to aid in diagnostics.

1.1. Requirements notation

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].

2. Use cases

2.1. Increasing the size of the ID space

The Header section of the DNS Message format contains a 16-bit ID field (see [RFC1035, Section 4.1.1 [RFC1035]). This field is used to match replies to their queries. If an attacker is able to predict this field he may be able to spoof a reply and perform a DNS cache poisining attack. By inserting arbritary data into the ECHO OPTION-DATA in a query (and checking that the same data is returned in the response), an iterative resolver can protect itself against this type of attack. Note that the resolver needs to add additional steps to protect against a downgrade attack. This technique does not protect against a man in the middle attack.

To avoid maintaining additional state for each query, the sender can algorithmically generate the ECHO OPTION-DATA. As an example it could generate this data field by calculating a hash over the concatenation of various fileds (such as the QNAME and the ID field) and a secret.

3. ECHO Option format

The OPTION-CODE for the ECHO option is TBD.

The OPTION-DATA for the ECHO option is an opaque byte string, the semantics of which are deliberately left outside the protocol.

The OPTION-DATA only has meaning to the sender. The software that generates the response or any intermediate device SHOULD NOT try and infer anything from the data.

3.1. Presentation format

User interfaces MUST read and write the contents of the ECHO option as a sequence of hexadecimal digits, two digits per payload octet. The ECHO payload is binary data. Any comparison between ECHO payloads MUST be a comparison of the raw binary data. Copy operations MUST NOT assume that the raw payload is null-terminated.

4. IANA Considerations

The IANA is requested to assign a value from the "DNS EDNS0 Options" registry, setting the name to be "ECHO" and referencing this document.

The code for the option should be TBD.

5. Security Considerations

A common form of denial of service attack is the reflected DNS amplification attack. In this attack an attacker spoofs DNS requests from the victim that will result in a much larger reply (the amplification factor). While the attacker could include a large amount of data in the ECHO payload of the spoofed DNS requests, this doesn't create any amplification.

The ECHO option could be used for DNS tunneling and exfiltration of data.

6. Acknowledgements

The authors wish to thank some folk.

7. References

7.1. Normative References

[IANA.AS_Numbers]
IANA, "Autonomous System (AS) Numbers",
<http://www.iana.org/assignments/as-numbers>.

[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.

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

7.2. Informative References

[I-D.ietf-sidr-iana-objects]
Manderson, T., Vegoda, L., and S. Kent, "RPKI Objects issued by IANA", draft-ietf-sidr-iana-objects-03 (work in progress), May 2011.

Appendix A. Changes / Author Notes.

[RFC Editor: Please remove this section before publication]

Changes from $undefined to -00.

- Initial document generation.

Notes / references:

- rfc2671.txt - Extension Mechanisms for DNS (EDNS0)
- rfc5001.txt - DNS Name Server Identifier (NSID) Option

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Roy Arends
Nominet
Minerva House, Edmund Halley Road
Oxford OX4 6LB
UK

Email: roy@nominet.org.uk