The EDNS(0) Padding Option
draft-mayrhofer-edns0-padding-01

Abstract

   This document specifies the EDNS(0) 'Padding' option, which allows
   DNS clients and servers to pad request and response messages by a
   variable number of octets.

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 February 15, 2016.

Table of Contents

1. Introduction

The Domain Name System (DNS) [RFC1035] was specified to transport DNS
packets in clear text form. Since this can expose significant
amounts of information about the internet activities of an end user,
the IETF has undertaken work to provide confidentiality to DNS
transactions (see the DPRIVE WG). Encrypting the DNS transport is
considered as one of the options to improve the situation.

However, even if both DNS query and response packets were encrypted,
meta data of these packets could be used to correlate such packets
with well known unencrypted packets, hence jeopardizing some of the
confidentiality gained by encryption. One such property is the
message size.

This document specifies the Extensions Mechanisms for DNS (EDNS(0))
"Padding" Option, which allows to artificially increase the size of a
DNS message by a variable number of bytes, significantly hampering
size-based correlation of the encrypted packet.

2. Terminology

The terms "Requestor", "Responder" are to be interpreted as specified
in [RFC6891].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
[RFC2119].

3. The 'Padding' Option

   The EDNS(0) [RFC6891] specifies a mechanism to include new options in
   DNS packets, contained in the RDATA of the OPT meta-RR. This
   document specifies the 'Padding' option in order to allow clients and
   servers pad DNS packets by a variable number of bytes. The 'Padding'
   option MUST occur at most once per OPT meta-RR.

   The figure below specifies the structure of the option in the RDATA
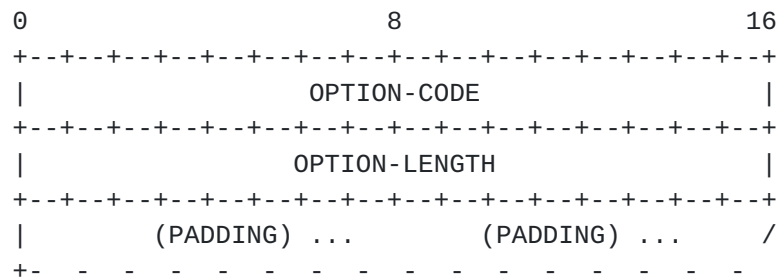   of the OPT RR:

```
                0                  8                 16
                +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
                |                 OPTION-CODE                   |
                +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
                |                OPTION-LENGTH                  |
                +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
                |       (PADDING) ...       (PADDING) ...    /
                +- - - - - - - - - - - - - - - - -
```

                               Figure 1

   The OPTION-CODE for the 'Padding' option is [[TODO-IANA]].

   The OPTION-LENGTH for the 'Padding' option is the size (in octects)
   of the PADDING. The minimum number of padding octects is 0.

   The PADDING octects MUST be set to 0x00. If a Responder detects non-
   0x00 octects in the padding of a query, a FORMERR (RCODE=1) MUST be
   returned.

4. Usage Considerations

   This document does not specify the actual amount of padding to be
   used, since this depends on the situation in which the option is
   used. However, padded DNS messages MUST NOT exceed the respective
   UDP payload size (see Section 6.2.3 and 6.2.4 of [RFC6891]).

   Responders MUST pad DNS responses when the respective DNS query
   included the 'Padding' option, unless doing so would violate the
   maximum UDP payload size.

   Responders MAY pad DNS responses when the respective DNS query
   indicated EDNS(0) support of the Requestor.

   Responders MUST NOT pad DNS responses when the respective DNS query
   did not indicate EDNS(0).

5. IANA Considerations

   IANA is requested to assign an EDNS Option Code (as described in
   Section 9 of [RFC6891]) for the 'Padding' option specified in this
   document.

6. Security Considerations

   Padding DNS packets obviously increases their size, and will
   therefore lead to increased traffic, can lead to increased number of
   truncated packets when used over UDP-based transport.

   The use of the EDNS(0) Padding provides only a benefit when DNS
   packets are not transported in clear text. Implementations therefore
   SHOULD avoid using this option if the DNS transport is not encrypted.

   The payload of the 'Padding' option could be used as a covert
   channel. In order to prevent this, padding octets are required to be
   set to 0x00. It shall be noted that variations in the OPTION-SIZE
   itself could still be abused for expensive and low-bandwith covert
   communication.

7. Acknowledgements

   This document was inspired by a discussion with Daniel Kahn Gillmor
   during IETF93, as an alternative to the proposed padding on the TLS
   layer.

8. Changes

8.1. draft-mayrhofer-edns0-padding-01

   Changed minimum padding size to 0, rewrote Usage Considerations
   section, extended Security considerations section

8.2. draft-mayrhofer-edns0-padding-00

   Initial version

9. Normative References

   [RFC1035] Mockapetris, P., "Domain names - implementation and
              specification", STD 13, RFC 1035, DOI 10.17487/RFC1035,
              November 1987, <http://www.rfc-editor.org/info/rfc1035>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms
              for DNS (EDNS(0))", STD 75, RFC 6891,
              DOI 10.17487/RFC6891, April 2013,
              <http://www.rfc-editor.org/info/rfc6891>.

Author's Address

   Alexander Mayrhofer
   nic.at GmbH
   Karlsplatz 1/2/9
   Vienna 1010
   Austria

   Email: alex.mayrhofer.ietf@gmail.com