Network Working Group   A. Mayrhofer
Internet-Draft   nic.at GmbH
Intended status: Standards Track   March 6, 2016
Expires: September 7, 2016

The EDNS(0) Padding Option
draft-ietf-dprive-edns0-padding-03

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 will expire on September 7, 2016.

Copyright Notice

Table of Contents

1. Introduction

The Domain Name System (DNS) [RFC1035] was specified to transport DNS messages 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 messages were encrypted, meta data could still be used to correlate such messages with well known unencrypted messages, 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, hampering size-based correlation of the encrypted message.

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 (and hence, at most once per message).

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 12.

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

The PADDING octets SHOULD be set to 0x00. Other values MAY be used; for example, in cases where there is a concern that the padded message could be subject to compression before encryption. PADDING octets of any value MUST be accepted in messages received.

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 number of octets specified in the Requestor's Payload Size field encoded in the RR Class Field (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 and the 'Padding' option was not included.

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

5. IANA Considerations

IANA has assigned EDNS Option Code 12 for Padding.

IANA is requested to update the respective registration record by changing the Reference field to [[THISRFC]] and the Status field to 'Standard'.

6. Security Considerations

Padding DNS packets obviously increases their size, and will therefore lead to increased traffic.

The use of the EDNS(0) Padding only provides a benefit when DNS packets are not transported in clear text. Further, it is possible EDNS(0) Padding may make DNS amplification attacks easier. Implementations therefore MUST NOT use this option if the DNS transport is not encrypted.

Padding length might be affected by lower-level compression. Therefore (as described in Section 3.3 of [RFC7525]), implementations and deployments SHOULD disable TLS-level compression.

The payload of the 'Padding' option could (like many other fields in the DNS protocol) be used as a covert channel.

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. Allison Mankin, Andreas Gustafsson, Christian Huitema, Jinmei Tatuya and Shane Kerr suggested text for this document.

8. Changes

Note to RFC Editors: Please remove this whole section before publication

8.1. draft-ietf-dprive-edns0-padding-03

Fixed typo in Acknowledgements, added Shane. Do not use over unencrypted transport is now a MUST. Logic around when responders may send the option clarified. Reduced "hampering" claim in introduction.

8.2. draft-ietf-dprive-edns0-padding-02

Clarified that changes section is to be removed before publication. Clarified that both Requestors and Responders are to ignore padding contents. changed text about non-zero padding contents based on WGLC comments. removed security considerations about truncation based on WGLC comment. added more acknowledgements. replaced "packets" with "messages" where appropriate.

8.3. draft-ietf-dprive-edns0-padding-01

Fixed 'octects' typo. Changed 'covert channel' text to align with allowing non-0x00 padding. changed IANA considerations - assigned option code is 12. Changed field definitions to allow for non-0x00 padding, removed FORMERR requirement. referenced rfc7525 in security considerations. added acknowledgements.

8.4. draft-ieft-dprive-edns0-padding-00

Adopted by WG. Changed text about message size limit based on feedback.

8.5. draft-mayrhofer-edns0-padding-01

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

8.6. draft-mayrhofer-edns0-padding-00

Initial version

9. References

9.1. 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>.

9.2. Informative References

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <http://www.rfc-editor.org/info/rfc7525>.

Author's Address

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

Email: alex.mayrhofer.ietf@gmail.com