Internet Engineering Task Force (IETF)
Request for Comments: 7830
Category: Standards Track
ISSN: 2070-1721

A. Mayrhofer
nic.at GmbH

May 2016

The EDNS(0) Padding Option

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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7830.

Table of Contents

1. Introduction

The Domain Name System (DNS) [RFC1035] was specified to transport DNS messages in cleartext 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 working group). Encrypting the DNS transport is considered one of the options to improve the situation.

However, even if both DNS query and response messages were encrypted, metadata 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 DNS clients and servers 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" and "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 to 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:

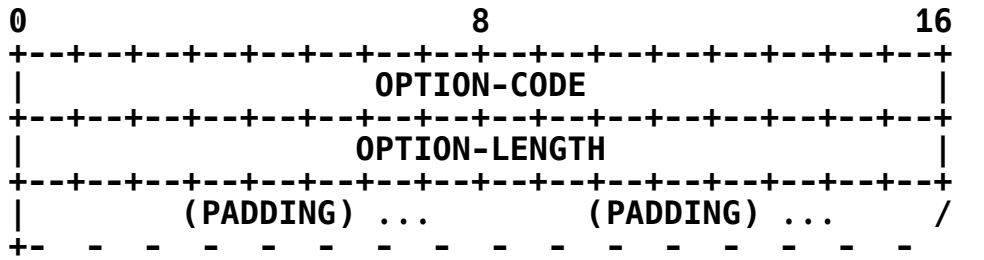

Figure 1

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 the 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 Sections 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 Option Code 12 for "Padding" in the "DNS EDNS0 Option Codes (OPT)" registry.

IANA has updated the respective registration record by changing the Reference field to RFC 7830 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 cleartext. Further, it is possible that EDNS(0) padding may make DNS amplification attacks easier. Therefore, implementations 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 compression at the Transport Layer Security (TLS) level.

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

7. References

7.1. 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>.

7.2. 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>.

Acknowledgements

This document was inspired by a discussion with Daniel Kahn Gillmor during IETF 93, 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.

Author's Address

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

Email: alex.mayrhofer.ietf@gmail.com