

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 8, 2017

A. Mayrhofer
nic.at GmbH
December 5, 2016

Padding Policy for EDNS(0)
draft-ietf-dprive-padding-policy-00

Abstract

[RFC 7830](#) specifies the EDNS0 'Padding' option, but does not specify the amount of padding to be used in specific applications. This memo lists the possible options ("Padding Policies"), discusses the implications of each of these options, and provides implementation guidance.

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 June 8, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	2
3.	General Guidance	2
4.	Padding Strategies	3
4.1.	No Padding	3
4.2.	Fixed Length Padding	3
4.3.	Block Length Padding	4
4.4.	Random Length Padding	4
4.5.	Random Block Length Padding	5
5.	IANA Considerations	5
6.	Security Considerations	5
7.	Changes	5
7.1.	draft-ietf-dprive-padding-policy-00	6
7.2.	draft-mayrhofer-dprive-padding-profiles-00	6
8.	Normative References	6
	Author's Address	6

[1.](#) Introduction

[RFC 7830](#) [[RFC7830](#)] 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 encrypted DNS messages.

However, [RFC 7803](#) deliberately does not specify the actual amount of padding to be used. This memo discusses options regarding the actual size of padding, and lists advantages and disadvantages of each of these "Padding Strategies".

[2.](#) Terminology

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.](#) General Guidance

Padding messages does not have any semantic impact on the DNS protocol. However, the amount of (possible) padding does depend on the circumstances under which a DNS message is created, specifically the maximum message length as dictated by protocol negotiations. Therefore, in order to not impact the possibility to add other EDNS options, "Padding" MUST be the last EDNS option applied before a DNS message is sent.

Especially in situations with scarce computing and networking resources such as long-life battery powered devices, the tradeoff between significantly increasing the size of DNS messages by generous padding and the corresponding gain in confidentiality must be carefully considered.

4. Padding Strategies

This section is a non-exhaustive list of strategies with regards to choosing the appropriate padding length.

4.1. No Padding

In the "No Padding" policy, the EDNS0 Padding option is not used, and the size of the final (actually, "non-padded") message obviously corresponds exactly to the size of the unpadded messages. Even though this "non-policy" could seem out of choice in this list, it needs to be considered for cases when either of the parties (client or server) does not apply padding, while the other party does.

Note that following this "policy" is required if the message size of the unpadded message does not allow for the Padding option to be included (less than 4 octets message space left). Therefore, this "non-policy" is listed here for the sake of completeness.

Advantages: The only advantage of this approach is that this "policy" requires no additional resources on client, server and network side.

Disadvantages: The original size of the message remains unchanged, hence this approach adds no additional entropy

TODO: Recommend that this policy MUST NOT be used unless message size disallows the use of Padding.

4.2. Fixed Length Padding

In fixed length padding, a sender chooses to pad each message with a padding of constant length.

Options: Actual length of padding

Advantages: Since the padding is constant in length, this policy is very easy to implement, and at least ensures that the message length diverges from the length of the original packet (even only by a fixed value)

Disadvantage: Obviously, the amount of padding easily discoverable from a single decrypted message. When a public DNS server applies

this policy, the length of the padding hence must be assumed to be public knowledge. Therefore, this policy is almost as bad as the "No Padding" option described above.

4.3. Block Length Padding

In Block Length Padding, a sender pads each message so that its padded length is a multiple of a chosen block length. This creates a greatly reduced variety of message lengths. An implementor needs to consider that even the zero-length EDNS0 Padding Option increases the length of the packet by 4 octets.

Options: Block Length - values between 16 and 128 (Discuss!) octets seem reasonable

Advantages: This policy is reasonably easy to implement, reduces the variety of message ("fingerprint") sizes significantly, and does not require a source of (pseudo) random numbers, since the amount of padding can be derived from the actual (unpadded) message.

Disadvantage: Given an unpadded message and the block size of the padding (which is assumed to be public knowledge once a server is reachable), the size of a message can be predicted. Therefore, the minimum and maximum length of the unpadded message is known.

TODO: Recommended policy?

4.4. Random Length Padding

When using Random Length Padding, a sender pads each message with a random amount of padding. Due to the size of the EDNS0 Padding Option itself, each message size is hence increased by at least 4 octets. The upper limit for padding is the maximum message size. However, a client or server may choose to impose a lower maximum padding length.

Alternatively, pad a certain percentage of "remaining space"?

Options: Maximum (and eventually minimum) padding length.

Advantages: This policy should create the best "distribution" of message sizes

Disadvantage: This policy requires a good source of (pseudo) random numbers which keeps up with the required message rates. Especially on busy servers, this could be a significant hindrance.

TODO: Recommendation - this is (at first glance) the best policy, but requires significant effort

4.5. Random Block Length Padding

This policy combines Block Length Padding with a random component. Specifically, a sender randomly chooses between a few block lengths and then applies Block Length Padding based on the chosen block length. The random selection of block length might even be reasonably based on a "weak" source of randomness, such as the transaction ID of the message.

Options: Number of size of the set of Block Lengths, source of "randomness"

Advantages: Compared to Block Length Padding, this creates more variety in the resulting message sizes for a certain individual original message length. Also, compared to "Random Length Padding", it might not require a "full blown" random number source.

Disadvantage: Requires more implementation effort compared to simple Block Length Padding

TODO: Recommend over simple Block Length Padding?

5. IANA Considerations

This document has no considerations for IANA.

6. Security Considerations

The choice of the right padding policy (and the right parameters for the chosen policy) has a significant impact on the resilience of encrypted DNS against size-based correlation attacks. Therefore, any implementor of EDNS0 Padding must carefully consider the chosen policy and its parameters.

A client's carefully chosen Padding policy may be without effect if the corresponding server does not apply an ineffective (or no) Padding policy on the response packets. Therefore, a client applying Padding may want to choose a DNS server which does apply at least an equally effective Padding policy on responses.

7. Changes

[7.1. draft-ietf-dprive-padding-policy-00](#)

Initial (mostly unmodified) WG version. Changed "Profile" to "Policy" to avoid confusion with the (D)TLS profiles document.

[7.2. draft-mayrhofer-dprive-padding-profiles-00](#)

Initial version

8. Normative References

[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>>.

[RFC7830] Mayrhofer, A., "The EDNS(0) Padding Option", [RFC 7830](#), DOI 10.17487/RFC7830, May 2016, <<http://www.rfc-editor.org/info/rfc7830>>.

Author's Address

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

Email: alex.mayrhofer.ietf@gmail.com

