Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 24, 2016

A. Mayrhofer
nic.at GmbH
July 23, 2015

The EDNS(0) Padding Option
draft-mayrhofer-edns0-padding-00

Abstract

This document specifies the EDNS0 'Padding' option, allowing DNS clients and servers to pad request and response packets by a variable number of bytes. This is to be used together with encrypted DNS transports in order to impede message-size based correlation attacks on the confidentiality of messages.

Status of This Memo

This Internet-Draft will expire on January 24, 2016.

Copyright Notice

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 current 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, and hence jeopardizing some of the confidentiality gained by encryption. One such property is the message size.

Size-based correlation of encrypted packets can be avoided by padding application messages with additional data. This document specifies the Extensions Mechanisms for DNS (EDNS(0)) "Padding" Option, which allows to artificially increase the size of a DNS packet by a variable number of bytes, in order to prevent size-based correlation once the packet is encrypted.

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. The 'Padding' Option

The EDNS0 specification [RFC6891] specifies a way to include new options for DNS packets, contained in the RDATA of the OPT meta-RR. This document specifies one such new 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 1.

The PADDING octects SHOULD be set to 0x00 (TODO: Discuss - together with compression in the encrypted transport, this could weaken the padding).

4. Client Considerations

A client SHOULD use the 'Padding' option in a DNS query (QR=0) only when transport of the DNS packets is encrypted. Note that there might be situations (such as bump-in-the-wire encryption) where a client is unable to identify whether or not encryption is being performed.

This document is silent on the length of the padding a client should use, since this is believed to be subject of the specification of an actual encrypted DNS transport (and might depend on its properties).

5. Server Considerations

A server MUST use the 'Padding' option in a DNS response (QR=1) only when that response correlates to a query that contained the 'Padding' option.

This document is silent on the length of the padding a server should use, since this is believed to be subject of the specification of an actual encrypted DNS transport.

6. 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.

7. Security Considerations

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

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.

8. 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.

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: alexander.mayrhofer@nic.at