Dprive Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 16, 2021

Z. Yan
CNNIC
G. Geng
Jinan University
Y. Liu
CAICT
X. Zhang
Shandong Computer Science Center
X. Zhu
Shandong Institute of Big Data

December 13, 2020

Indication of Local DNS Privacy Service During User Access
draft-yan-dprive-local-service-indication-04

Abstract

This document aims to support the indication of privacy service capability of recursive resolver during the end-user accesses the network.

Requirements Language

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

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 https://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 16, 2021.

Table of Contents

1. Introduction

In order to enhance the privacy protection in DNS, several solutions have been developed to support the encrypted communications between stub and recursive resolvers, such as DNS-over-DTLS [RFC8094], DNS-over-TLS [RFC7858], DNS-over-QUIC and so on. However, a scheme is needed in order to explicitly make the end-user (stub resovler) be aware of the types of privacy service supported by the recursive resolver in order to avoid the blind attempt by the end-user and support the user to bootstrap the preferred privacy protocol more easily. This can be achieved during the user initial access, using extended DHCPv6 or ICMPv6 to configure its recursive resolver with related information (only IPv6 scenario is considered herein).

2. ICMPv6 based case

The "Recursive DNS Server Option" is defined in [RFC8106] to support the user to configure DNS recursive resolver in the IPv6 SLAAC mode. Then a 4-bit (for example) space (denoted as "Cap." field) in the Reserved field of "Recursive DNS Server Option" can be used to indicate the privacy service of the corresponding recursive resolver specified in the field of "Addresses of IPv6 Recursive DNS Servers". However, if this function is used, the "Addresses of IPv6 Recursive

DNS Servers" should contain only the recursive resolver(s) with the same privacy service capability indicated by the corresponding "Cap." field. How to code the "Cap." field will be detailed further.

3. DHCPv6 based case

The "DNS Recursive Name Server option" is defined in [RFC3646] to support the user to configure DNS recursive resolver in the IPv6 DHCP [RFC4339] mode. However, [RFC3646] did not reserve extra space, a new option should be defined which is conjunctively used with "DNS Recursive Name Server option". It is defined as "DNS Recursive Server Privacy option" and the format is shown in Figure 1.

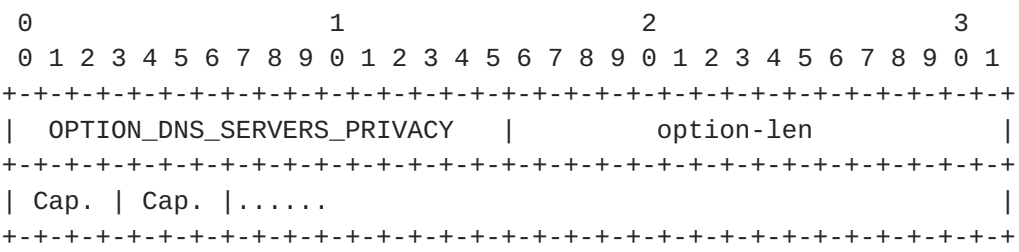

Figure 1: DNS Recursive Server Privacy option

- option-code: OPTION_DNS_SERVERS_PRIVACY

- option-len: Length of the list of privacy service capability of DNS recursive name servers in octets; must be a multiple of 4 (for example).

- Capability: The 4-bit (for example) space (denoted as "Cap." field) is used to indicate the privacy service of the corresponding recursive resolver specified in the field of DNS-recursive-name-server in the DNS Recursive Name Server option.

The DNS Recursive Server Privacy option should be used conjunctively with the DNS Recursive Name Server option and the order of "Cap." fields in the DNS Recursive Server Privacy option must be corresponding to the server order specified in the DNS Recursive Name Server option.

4. Security considerations

TBA

5. 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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, DOI 10.17487/RFC3646, December 2003, <https://www.rfc-editor.org/info/rfc3646>.

[RFC4339] Jeong, J., Ed., "IPv6 Host Configuration of DNS Server Information Approaches", RFC 4339, DOI 10.17487/RFC4339, February 2006, <https://www.rfc-editor.org/info/rfc4339>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

Appendix A. Acknowledgments

This work was supported by Beijing Nova Program of Science and Technology under grant Z191100001119113.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
China

EMail: yan@cnnic.cn

Guanggang Geng
Jinan University
No.601, West Huangpu Avenue
Guangzhou 510632
China

EMail: gggeng@jnu.edu.cn

Yang Liu
CAICT
No.52, Huayuanbeilu
Beijing 100191
China

EMail: liuyang7@caict.ac.cn

Xinchang Zhang
Shandong Computer Science Center
No.19 Keyuan Road, Lixia District
Jinan, 250014
P.R. China

EMail: xincha.zhang@gmail.com

Xiaomin Zhu
Shandong Institute of Big Data
7/F, building 7, Shun Tai Plaza, No.2000, Shun Hua Road, hi-tech Zone
Jinan, 250014
P.R. China

EMail: zhuxiaomin@ict.ac.cn