Indication of Local DNS Privacy Service During User Access
draft-yan-dprive-local-service-indication-00

Abstract

This document aims to support the indication of privacy service of recursive resolver during the user access.

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 January 22, 2020.

Copyright Notice

Copyright (c) 2019 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 (https://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. ICMPv6 based case ........................................ 2
3. Other configuration cases ................................. 2
4. Security considerations ................................. 3
5. Normative References ................................. 3
6. Authors’ Addresses ................................. 3

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 user aware of the privacy service supported by the recursive resolver in order to avoid the blind attempt by the 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 here).

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 an x-bit flag 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 one address of recursive resolver. What the size of "x" and how to specify the flag corresponding to the supported privacy service of the recursive resolver will be detailed further.

3. Other configuration cases

The procedures based on the DHCPv6 or other configuration protocols [RFC3646][RFC4339]will also be considered further.
4. Security considerations

TBA

5. Normative References


Authors’ Addresses

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

EMail: yan@cnnic.cn