Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 27 April 2022

B. Dickson
GoDaddy

24 October 2021

Resource Record for Signaling Transport for DNS to Authority Servers
draft-dickson-dprive-dnst-00

Abstract

This Internet Draft proposes an RRTYPE to signal explicit support for transport types for DNS service. This new RRTYPE is "DNST". The available transports to signal are TCP and UDP on port 53 (DNS), and DoT (DNS over TLS) transport using TCP port 853.

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 27 April 2022.

Copyright Notice

Copyright (c) 2021 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. Conventions and Definitions

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Background

DNS over TLS is defined in [RFC7858]. However, there is no explicit signaling for when DoT should be used. Without explicit signaling, there is no protection against downgrade attacks by an on-path attacker.

4. Remove Before Publication

Notes on design decisions, including the decision NOT to use an SVCB-compatible format:

* NS records MUST point to non-CNAME records. Thus, there is no need for the SVCB "Alias-form" behavior. DNST does not support aliasing,

* DNST allows for explicit rejection of default transport (UDP/53 and TCP/53)

* DNST allows explicit signaling of DoT

* There is no need for alternate port numbers for UDP or TCP port 53, or for DoT port 853.

* There is no need for DoH, since the expected clients are limited to DNS resolvers.

5. DNS Transport RRTYPE

The solution to this problem is to introduce a method for explicit signaling for when DoT is available. When combined with TLSA [RFC6698] records for the corresponding DNS server name, any client wishing to use DoT is able to know that it is available, and can detect and avoid any attempts at transport downgrade.

This document defines the RRTYPE value {TBD} with mnemonic name DNST ("DNS Transport"). This consists of a set of flags indicating supported transport for the DNS server at the owner name. The flag bits represent transports:

* UDP on port 53

* TCP on port 53

* DoT (DNS over TLS) on port 853

6. Restrictions

The DNST record may occur anywhere, including at the apex of a DNS zone, and may co-exist with any other type that also permits other types.

7. Wire Format

The RDATA wire format is an 8-bit octet of flag bits.

| UDP | TCP | DOT | 5 unused bits |

8. Presentation Format

OWNER CLASS TTL DNST [UDP] [TCP] [DOT]

At least one of the transport types must be present.

9. Additional Processing

The authoritative server MAY/SHOULD return both the DNST record(s) and any/all A and AAAA records with the same owner name. This reduces the number of queries the resolver would otherwise have to make (i.e. two additional queries for A and AAAA record types).

10. Security Considerations

The DNST record MUST be in a DNSSEC-signed zone. This ensures protection against downgrade attacks on the transport signaling.

11. IANA Considerations

IANA is directed to add a new record to the DNS RRTYPES table to add the entry "DNST" with value "TBD", referencing this document.

12. Normative References

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

13. Informative 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>.

Appendix A. Acknowledgments

Thanks to everyone who helped create the tools that let everyone use Markdown to create Internet Drafts, and the RFC Editor for xml2rfc.

Thanks to Dan York for his Tutorial on using Markdown (specificially mmark) for writing IETF drafts.

Thanks to YOUR NAME HERE for contributions, reviews, etc.

Author's Address

Brian Dickson
GoDaddy

Email: brian.peter.dickson@gmail.com