Signalling That an Authoritative DNS server offers DoT
draft-levine-dprive-signal-00

Abstract

DNS resolvers that wish to use DNS over TLS to authoritative servers (ADoT) need some way to tell whether server offers DoT. This document describes some ways that a server might signal that it uses DoT.

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 May 5, 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.
1. Introduction

The Domain Name System [RFC1034] [RFC1035] uses a directed presumably acyclic graph of servers to provide authoritative answers to queries. The link from one server to the next is provided by an NS record in the zone on the upper server that points to the lower server. For zones signed with DNSSEC, the upper server zone contains DS records that contain hashes of signing keys in DNSKEY records in the zone on the lower server.

2. General observations

In several of the following schemes, the client probes the server to see whether it offers ADoT. In those cases, the client presumably remembers what servers it’s probed so there’s only one probe per server.

The probe query would generally use query minimization to limit leakage of the requested name. Even so, if a server handles many zones, this leaks the name of the zone being probed.

Some zones have servers run by multiple operators. (The DNS root is a well known example.) It is possible that some of the servers will offer ADoT and some will not. Some of the schemes below handle per-server signals, some don’t.

3. Signaling methods

This is a working list of possible signalling methods. Just because they’re in the list doesn’t mean that anyone thinks they’re a good idea.

3.1. EDNS0 option

We define a new EDNS0 option edns-adot. The client sends an edns-adot option in its request, and the server responds with a value of 0 or 1 to say whether it supports ADoT. The option could be served by
the upper level server along with the NS records, which avoids the extra probe, or by the lower level server.

This is easy to implement, but since the OPT isn’t signed, it’s subject to downgrade attacks. If served by the upper level server, there’s no per-server indication, but also no extra round trip.

3.2. DNSKEY

A DNSKEY [RFC4034] at the apex of the zone signals that ADoT is available. The simplest approach would be to use one of the unassigned DNSKEY flags to indicate that the zone is expected to be served over ADoT. This is resistant to downgrade, since the DNSKEY is signed, but there’s no per-server indication. DNSSEC clients have to fetch the DNSKEY records anyway so there’s no extra round trip. Since nobody has ever used DNSKEY records with flag values other than 0, 256, and 257, some software may fail if it sees other flag values.

Another approach is to add a pseudo-algorithm ADOT for which the public key value is the name(s) of the servers expected to support ADoT. This provides per-server indication, and is backward compatible since DNSSEC clients already need to ignore unknown algorithms, but it makes the DNS Camel sad.

3.3. Special server names

Any server that supports ADoT has a name starting with the four characters "XS--". All names starting with two letters other than "XN" and two dashes were reserved when IDNs were invented, so these names are unlikely to collide with any existing names. Note that these are not IDNs, they’re just funny looking ASCII names, and you can’t do "XN--XS--blah" or anything like that.

This is backward compatible, downgrade resistant, needs no extra round trip, and allows per-server signals. It doesn’t allow server names to be IDNs which should not be a big problem since DNS server names are not generally shown to users, although it may confuse people who believe that anything with two dashes must be an IDN.

The Camel is also not crazy about it.

4. References - Normative


Author’s Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY  14886

Email: standards@taugh.com
URI:  http://jl.ly