Compact Denial of Existence in DNSSEC

Shumon Huque, Christian Elmerot, Ólafur Guðmundsson

November 10th 2023

DNS Operations Working Group

Internet Engineering Task Force (IETF) 118 Meeting

Prague, Czechia

Current version: 01

- Versioned draft:
  - https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-compact-denial-of-existence-01
- Datatracker link:
  - https://datatracker.ietf.org/doc/draft-ietf-dnsop-compact-denial-of-existence/

Implementation Status section

- Note Cloudflare’s deployment of NXNAME using private RR type 65283

NS1 will switch to NXNAME sentinel type soon

[dns-operations@dns-oarc.net]
Subject: NS1 changing compact NSEC for NXNAME
From: Jan Včelák jv at fcelda.cz
Tue Nov 7 23:05:41 UTC 2023

NS1 is going to deploy a change to the Compact Denial of Existence in DNSSEC which modifies the signaling for empty non-terminals and non-existent names in the NSEC bit map.

Currently, we include TYPE65281 in the NSEC bit map for empty non-terminals. We are going to remove that bit and instead set TYPE65283 in the NSEC bit map for non-existent names.

[...]

Only specify NXNAME type

- Consensus is to only specify the NXNAME type.
- The ENT type will be retired, and mentioned for historical reasons.
- Only one opposing view (keep ENT, or only specify ENT)
  - Only ENT does not allow us to distinguish NXDOMAIN across different implementations of online signing.

Section 3.4 - Explicit queries for NXNAME

- Although nothing should be explicitly querying this pseudo RR type, we clarify what the response should be if such queries are received.
- Treat as normal query type: 2 cases:
  - Query at name that exists (including at an Empty Non Terminal):
    - Standard NODATA response, enumerating types that exist in the NSEC bitmap
  - **Query at name that does not exist:**
    - **NODATA response with NXNAME deliberately excluded from the NSEC bitmaps**.
    - Reason: including NXNAME in the type bitmap when the query type itself is NXNAME, may cause resolvers to SERVFAIL & retry - the response's NSEC record claimed data of type NXNAME existed at the name, yet the Answer section is empty.
    - But loss of NXDOMAIN signal
- Treat as meta-type & return error (but type space ambiguity; private space?)

RCODE 3 restoration: DO=0 queries

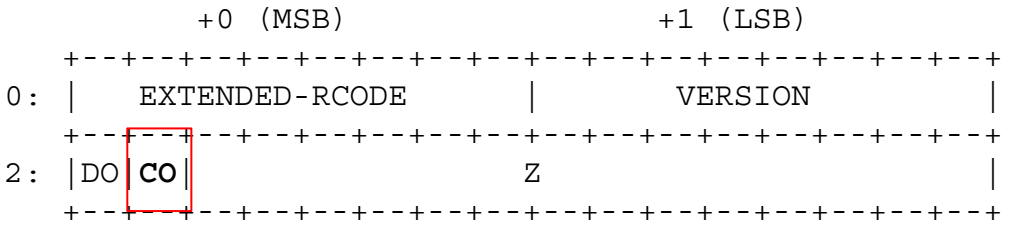
- Authoritative Servers
  - Could just supply a normal NXDOMAIN response.
  - Is it worth it though, since most modern resolver always send DO=1 queries?
  - And DNSSEC aware resolvers are required to send DO=1:
    - From RFC 3225, Section 3: *“A recursive DNSSEC-aware server MUST set the DO bit on recursive requests, regardless of the status of the DO bit on the initiating resolver request.”*
- Iterative Resolvers/Forwarders etc
  - Recognize the NXNAME signal and restore NXDOMAIN in the RCODE field of responses it sends back to DO=0 clients. (Draft already mentions this.)
  - Additional cache management measures may be needed (tagging NXNAME enhanced responses for differential treatment to downstream queriers).

Signaled RCODE 3 Restoration for DO=1 queries

- Define new “Compact Answers OK” EDNS header flag (“CO”)
- If a DO=1 querier also sets CO=1, then a Compact Denial cognizant DNS server can send the NXNAME enhanced NODATA response, **and** additionally set RCODE=NXDOMAIN (3)
  - For an authority server this is straightforward.
  - For an iterative resolver, they would have to examine the NXNAME signal in cached data, and then:
    - if downstream querier sets Compact Answers OK, return signed NODATA with RCODE=3
    - if downstream querier does not set it, returned signed NODATA with RCODE=0 (NOERROR) - basically the same answer as today without signaling.

5.1. Signaled Response Code Restoration

This section describes an **optional but recommended scheme** to permit signaled restoration of the NXDOMAIN RCODE for DNSSEC enabled responses. **A new EDNS0 [RFC6891] header flag is defined in the 2nd most significant bit of the Z field in the EDNS0 OPT header. This flag is referred to as the "Compact Answers OK (CO)" flag.**



When this flag is sent in a query by a resolver, it indicates that the resolver will accept a signed NXNAME enhanced NODATA response for a non-existent name together with the response code field set to NXDOMAIN (3).

In responses to such queries, a Compact Denial authoritative implementing this signaling scheme, will set the Compact Answers OK EDNS header flag, and for non-existent names will additionally set the response code field to NXDOMAIN.

Repeat question: Applicability Statement?

- This spec standardizes a deployed existing practice.
- For new online signing implementers, should this spec advise them to only consider this mechanism if they have the specific requirements that necessitate it?
- And otherwise, recommend RFC4470 (White Lies/Minimally covering NSEC)? If so, they can avoid all the issues associated with missing or alternate NXDOMAIN signals.