Compact Denial of Existence in DNSSEC

Shumon Huque, Christian Elmerot, Ólafur Guðmundsson

March 18th 2024

DNS Operations Working Group

Internet Engineering Task Force (IETF) 118 Meeting

Brisbane, Australia

draft-ietf-dnsop-compact-denial-of-existence-03

- Updated sections:
  - Responses to explicit queries for NXNAME
  - Implementation Status
  - Security Considerations
  - IANA Considerations
- New section: “Updates to RFCs”

Section 3.4 - Explicit queries for NXNAME

- Treat NXNAME as a meta-type & return an error.
- FORMERR is proposed to match the behavior of existing resolvers like BIND and Unbound when they receive a query in the meta type range that has no existing response behavior defined.
- Resolvers specifically should return the error, and not forward the query upstream or attempt iterative resolution.

Update to RFC 4034

[RFC4034] Section 4.1.2, The Type Bit Maps Field, states the:

> * Bits representing pseudo-types MUST be clear, as they do not appear in zone data. If encountered, they MUST be ignored upon being read.

This paragraph is updated to the following:

> * Bits representing pseudo-types MUST be clear, as they do not appear in zone data. If encountered, they MUST be ignored upon being read. There is one exception to this rule for Compact Denial of Existence (RFC TBD), where the NXNAME pseudo-type is allowed to appear in responses to non-existent names.

(Should the exception be more general though??)

Update to RFC 4035

[RFC4035] Section 2.3, Including NSEC RRs in a Zone, states:

> * An NSEC record (and its associated RRSIG RRset) MUST NOT be the only RRset at any particular owner name. That is, the signing process MUST NOT create NSEC or RRSIG RRs for owner name nodes that were not the owner name of any RRset before the zone was signed. The main reasons for this are a desire for namespace consistency between signed and unsigned versions of the same zone and a desire to reduce the risk of response inconsistency in security oblivious recursive name servers. This concern only applies to implementations of DNSSEC that employ pre-computed signatures. There is an exception to this rule for online signing implementations of DNSSEC (e.g Minimally Covering NSEC, and Compact Denial of Existence (RFC TBD), where dynamically generated NSEC records can be produced for owner names that don't exist or are empty non-terminals.

Implementation Status section

- Both Cloudflare and NS1 have deployed NXNAME using private RR type code 65283
- They also plan to implement the optional RCODE restoration scheme (presently only prototype implementations of this feature exist)
- AWS Route53 is awaiting the spec to be near final and an official type code assigned.

IANA Considerations

- Explicitly request the first available number in the meta-types range for NXNAME (128)

Wrap up items

- Should DO=0 queries (be required to) respond with NXDOMAIN rcode
- Should response for explicit NXNAME query return a new EDE code?
- Discuss impacts on RFC8020/8198
- Submit Early Allocation requests for NXNAME type and CO flag?
- Ready for Working Group Last Call?