Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-ietf-dnsop-compact-denial-of-existence
Published: 9 May 2023
Intended Status: Standards Track
Expires: 10 November 2023
Authors: S. Huque (Salesforce) C. Elmerot (Cloudflare) O. Gudmundsson (Cloudflare)

Compact Denial of Existence in DNSSEC

Abstract

This document describes a technique to generate a signed DNS response on demand for a non-existent name by claiming that the name exists but doesn't have any data for the queried record type. Such answers require only one minimal NSEC record, allow online signing servers to minimize signing operations and response sizes, and prevent zone content disclosure.

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 10 November 2023.

Copyright Notice

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction and Motivation

RFC EDITOR: PLEASE REMOVE THIS PARAGRAPH BEFORE PUBLISHING: The source for this draft is maintained in GitHub at: https://github.com/shuque/id-dnssec-compact-lies

One of the functions of the Domain Name System Security Extensions (DNSSEC) [RFC9364] is "Authenticated Denial of Existence", i.e. proving that a DNS name or record type does not exist. Normally, this is done by means of signed NSEC or NSEC3 records. In the precomputed signature model, these records chain together existing names, or cryptographic hashes of them in the zone. In the online signing model, described in NSEC and NSEC3 "White Lies" [RFC4470] [RFC7129], they are used to dynamically compute an epsilon function around the queried name. A 'type bitmap' in the data field of the NSEC or NSEC3 record asserts which resource record types are present at the name.

The response for a non-existent name requires up to 2 signed NSEC records or up to 3 signed NSEC3 records (and for online signers, the associated cryptographic computation), to prove that (1) the name did not explicitly exist in the zone, and (2) that it could not have been synthesized by a wildcard.

This document describes an alternative technique, "Compact Denial of Existence" or "Compact Answers", to generate a signed DNS response on demand for a non-existent name by claiming that the name exists

but has no resource records associated with the queried type, i.e. it returns a NODATA response rather than an NXDOMAIN response. A NODATA response (which has a response code of NOERROR, and an empty ANSWER section) requires only one NSEC record matching the queried name. This has two advantages: the DNS response size is smaller, and it reduces the online cryptographic work involved in generating the response.

The use of minimally covering NSEC records also prevents adversaries from enumerating the entire contents of DNS zones by walking NSEC chains.

2. Distinguishing NXDOMAIN from Empty Non-Terminal Names

Since NODATA responses are generated for non-existent names, and there are no defined record types for the name, the NSEC type bitmap in the response will only contain "NSEC" and "RRSIG". Tools that need to accurately identify non-existent names in responses cannot rely on this specific type bitmap because Empty Non-Terminal (ENT) names (which positively exist) also have no record types at the name and will return exactly the same type bitmap.

Today, some specific implementations of Compact Answers avoid the NXDOMAIN identification problem by synthesizing the NSEC type bitmap for ENTs to include all record types supported except for the queried type. This has the undesirable effect of no longer being able to reliably determine the existence of ENTs, and of making the Type Bitmaps field potentially larger than it needs to be. It also has the potential to confuse validators and others tools that infer type existence from the NSEC record.

This document defines the use of a synthetic Resource Record type to signal the presence of a non-existent name. The mnemonic for this RR type is "NXNAME" and its type code is [TBD]. This RR type is added to the NSEC type bitmap for responses to non-existent names (in addition to the required RRSIG and NSEC types). The moniker NXNAME is chosen to clearly distinguish it from the response code NXDOMAIN.

No special handling of this RR type is required on the part of DNS resolvers. However, a resolver could optionally use the presence of the RR type to modify the response code in the answer it relays back to downstream non-validating clients from NODATA to NXDOMAIN.

An alternative way to distinguish NXDOMAIN from ENT is to define the synthetic Resource Record type for ENTs instead, as specified in [ENT-SENTINEL], and this has already been deployed in the field. This typically imposes less work on the server since NXDOMAIN responses are a lot more common than ENTs. And at the time it was deployed it allowed a common bitmap pattern ("NSEC RRSIG") to

identify NXDOMAIN across this and other implementations that returned a broad bitmap pattern for Empty Non-Terminals. However, the advantage of the NXNAME RR type is that it explicitly identifies NXDOMAIN responses, and allows them to be distinguished conclusively from potential ENT responses in other online signing NSEC implementations.

3. Generating Responses

This section describes various types of answers generated by authoritative servers implementing Compact Denial of Existence. At the current time, the compact denial scheme is only defined for NSEC. While it could support NSEC3 too, there is no benefit in introducing the additional complexity associated with it.

3.1. Responses for Non-Existent Names

When the authoritative server receives a query for a non-existent name in a zone that it serves, a NODATA response (response code NOERROR, empty Answer section) is generated with a dynamically constructed NSEC record with the owner name matching the queried name (QNAME).

The Next Domain Name field SHOULD be set to the immediate lexicographic successor of the QNAME. The Type Bit Maps field MUST only have the bits set for the following RR Types: RRSIG, NSEC, and NXNAME.

For example, a request for the non-existing name a.example.com would cause the following NSEC record to be generated (in DNS presentation format):

```
a.example.com. 3600 IN NSEC \000.a.example.com. RRSIG NSEC NXN
```

The NSEC record MUST have corresponding RRSIGs generated.

3.2. Responses for Non-Existent Types

When the authoritative server receives a query for a name that exists, but has no resource record sets associated with the queried type, it generates a NODATA response, with a dynamically constructed signed NSEC record in the Additional Section. The owner name of the NSEC record matches the queried name. The Next Domain Name field is set to the immediate lexicographic successor of the QNAME. The Type Bitmaps field lists the available Resource Record types at the name.

An Empty Non-Terminal is a special subset of this category, where the name has no resource record sets of any type (but has descendant names that do). For a query for an Empty Non-Terminal, the NSEC type bitmap will only contain RRSIG and NSEC. (Note that this is

substantially different than the ENT response in precomputed NSEC, where the NSEC record has the same type bitmap, but "covers" rather than matches the ENT, and has the Next Domain Name field set to the next lexicographic descendent of the ENT in the zone.)

3.3. Responses for Wildcard Matches

For wildcard matches, the authoritative server will provide a dynamically signed response that claims that the queried name exists explicitly. Specifically, the answer RR set will have an RRSIG record demonstrating an exact match (i.e. the label count in the RRSIG RDATA will be equal to the number of labels in the query name minus the root label). This obviates the need to include an NSEC record in the Authority section of the response that shows that no closer match than the wildcard was possible.

For a Wildcard NODATA match (where the queried name matches a wildcard but no data for the queried type exists), a response akin to a non-wildcard NODATA is returned. The Answer section is empty, and the Additional section contains a single NSEC record that matches the query name with a type bitmap representing the list of types available at the wildcard.

4. Operational Implications

For DNSSEC enabled queries, a signed zone at an authoritative server implementing Compact Answers will never return a response with a response code of NXDOMAIN. Tools that rely on accurately determining non-existent names will need to infer them from the presence of the NXNAME RR type in the type bitmap of the NSEC record in NODATA responses from these servers. The response code in the DNS header cannot be authenticated, so inferring the status of a response from signed data in the body of the DNS message is more secure.

Address lookup functions typically invoked by applications will continue to work, although extra invocations of these functions (and corresponding extra DNS queries) may be caused. For example, a NODATA response to the lookup of an AAAA record for a non-existent name, can cause an application to issue another query at the same name for an A record. Whereas a NXDOMAIN response to the first query would correctly suppress additional queries for other types at that name. Address lookup functions could be enhanced to examine the NSEC type bitmaps in responses to accurately determine non-existent names, however they would need to issue DNSSEC enabled queries and potentially deal with middleboxes interfering with the delivery of DNSSEC signed responses.

5. Response Code Substitution

For non-existent names, implementations should try wherever possible, to preserve the response code value of 3 (NXDOMAIN). This is generally possible for non-DNSSEC enabled queries, namely those which do not set the DNSSEC_OK EDNS flag. For such queries, authoritative servers could return a normal NXDOMAIN response. Additionally, a validating resolver that understands the NXNAME signal from an authoritative server could modify the response code from NOERROR to NXDOMAIN to downstream queriers that do not set the DNSSEC_OK flag.

TO EXPLORE: For DNSSEC enabled queries, preserving the NXDOMAIN response code likely needs the specification of a new EDNS signal ("Compact Answers OK") at additional complexity cost. Authoritative servers receiving queries with such a flag could return a Compact DNSSEC Answer with the response code set to NXDOMAIN. Resolvers could likewise return such an answer to their downstream DNSSEC enabled queriers that also set this flag. Validating resolvers would check that such responses either contained a traditional signed NXDOMAIN response or a signed NODATA response with the NXNAME signal.

6. Implementation Status

Cloudflare, NS1, and Amazon Route53 currently implement the base Compact Answers scheme. NS1 additionally implements the Empty Non-Terminal distinguisher in the NSEC type bitmap, using the private RR type code 65281. There are no implementations yet that use the NXNAME distinguisher RR type.

7. Security Considerations

Online signing of DNS records requires authoritative servers for the DNS zone to have access to the private signing keys. Exposing signing keys on Internet reachable servers makes them more vulnerable to attack.

Additionally, generating signatures on-demand is more computationally intensive than returning pre-computed signatures. Although the Compact Answers scheme reduces the number of online signing operations compared to previous techniques like White Lies, it still may make authoritative servers more vulnerable to computational denial of service attacks than pre-computed signatures. The use of signature algorithms (like those based on Elliptic Curves) that have a comparatively low cost for signing is recommended.

8. Acknowledgements

The Compact Answers technique (then called "Black Lies") was originally proposed in [BLACK-LIES] by F. Valsorda and O. Gudmundsson, and implemented by Cloudflare. The Empty Non-Terminal distinguisher RR type was originally proposed in [ENT-SENTINEL] by S. Huque. The NXNAME type is based on the FDOM type proposed in [NXDOMAIN-TYPE] by O. Gudmundsson and F. Valsorda.

9. IANA Considerations

IANA is requested to allocate a new DNS Resource Record type code for NXNAME in the DNS parameters registry, from the meta type range.

NXNAME	[TBD]	NXDOMAIN Distinguisher for Compact Denial of Exi

10. References

10.1. Normative References

[RFC4470] Weiler, S. and J. Ihren, "Minimally Covering NSEC Records and DNSSEC On-line Signing", RFC 4470, DOI 10.17487/RFC4470, April 2006, <https://www.rfc-editor.org/info/rfc4470>.

[RFC7129] Gieben, R. and W. Mekking, "Authenticated Denial of Existence in the DNS", RFC 7129, DOI 10.17487/RFC7129, February 2014, <https://www.rfc-editor.org/info/rfc7129>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

10.2. Informative References

[BLACK-LIES] Valsorda, F. and O. Gudmundsson, "Compact DNSSEC Denial of Existence or Black Lies", <https://tools.ietf.org/html/draft-valsorda-dnsop-black-lies>.

[ENT-SENTINEL] Huque, S., "Empty Non-Terminal Sentinel for Black Lies", <https://www.ietf.org/archive/id/draft-huque-dnsop-blacklies-ent-01.html>.

[NXDOMAIN-TYPE] Gudmundsson, O. and F. Valsorda, "Signaling NSEC record owner name nonexistence", <https://tools.ietf.org/html/draft-ogud-fake-nxdomain-type/>.

Authors' Addresses

Shumon Huque

Salesforce
415 Mission Street, 3rd Floor
San Francisco, CA 94105
United States of America

Email: shuque@gmail.com

Christian Elmerot
Cloudflare
101 Townsend St.
San Francisco, CA 94107
United States of America

Email: elmerot@cloudflare.com

Olafur Gudmundsson
Cloudflare
101 Townsend St.
San Francisco, CA 94107
United States of America

Email: olafur@cloudflare.com