Workgroup: Internet Engineering Task Force
Internet-Draft: draft-huque-black-lies-ent
Published: 27 July 2021
Intended Status: Informational
Expires: 28 January 2022
Authors: S. Huque
Salesforce

Empty Non-Terminal Sentinel for Black Lies

Abstract

The Black Lies method of providing compact DNSSEC denial of existence proofs has some operational implications. Depending on the specific implementation, it may provide no way to reliably distinguish Empty Non-Terminal names from names that actually do not exist. This draft describes the use of a synthetic DNS resource record type to act as an explicit signal for Empty Non-Terminal names and which is conveyed in an NSEC type bitmap.

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 28 January 2022.

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 and Motivation

One of the functions of the Domain Name System Security Extensions (DNSSEC) [RFC4033] [RFC4034] [RFC4035] 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 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, 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 associated name.

An alternative method, Black Lies [BLACKLIES], described in an expired Internet draft, provides more compact denial of existence proofs for online signers by relying on a clever hack. For non-existent names, it claims 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 sizes are smaller, and it reduces the online cryptographic work involved in generating the responses. By contrast, an NXDOMAIN response requires multiple records (up to 2 when using NSEC, and up to 3 when using NSEC3) 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.

The Black Lies method has some operational implications. Tools that rely on the correctness of the DNS response code (e.g. obtaining NXDOMAIN for non-existent domains) no longer work. Arguably, we should not be doing this anyway, since the response code in the DNS

header cannot be authenticated. This means that NXDOMAIN has to be "inferred" from signed records in the DNS response. Whether this inference can be reliably drawn depends on other details of the Black Lies implementation. A Black Lies NODATA response contains only "NSEC" and "RRSIG" in the NSEC type bitmap. This is not sufficient to infer NXDOMAIN though, because Empty Non-Terminal (ENT) responses (which positively exist) will return the exact same response. DNS operators often rely on precisely distinguishing NXDOMAIN from NODATA, including ENT responses (such as tools that prevent the creation of zone cuts or DNAME records at ENTs to avoid accidentally occluding names underneath them - these have been critical safety features of our DNS record provisioning systems).

Of the 3 implementations I've examined, NS1 (previously) and Amazon Route53 suffer from this NXDOMAIN/ENT indistinguishability. Cloudflare avoids this problem by synthesizing the NSEC type bitmap for ENTs to include all (?) RR Types they support, except for the queried type. This has the side effect though of no longer being able to reliably determine the existence of ENTs.

2. Synthetic Type for Empty Non-Terminal Names

This document proposes the use of a synthetic Resource Record type to signal the presence of an Empty Non-Terminal name. This RR type is added to the NSEC type bitmap for responses to ENTs. Currently, the deployed examples of this scheme are using the private RR type code 65281. So the resulting type bitmap would have "NSEC RRSIG TYPE65281". Should this document be published, a formal request for an RR type number could be made.

NS1 has implemented this scheme in their Managed DNS platform. The following is an example of a response to an Empty Non- Terminal name hosted on their service:

```
$ dig +dnssec +multi ent1.sfdcsd.net. A

; <<>> DiG 9.16.15 <<>> +dnssec +multi ent1.sfdcsd.net. A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53091
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;ent1.sfdcsd.net.       IN A

;; AUTHORITY SECTION:
ent1.sfdcsd.net.        3592 IN RRSIG NSEC 13 3 3600 (
                                20210712120255 20210710120255 44688 sfdc
                                lG/EJq0M1cs6vw0ragtvMV+B/Sd2CAPsxo1/WIOT
                                /QxukD5k8AeygmWYKnrR9jdb2SnXBxFEQss/mTSA
ent1.sfdcsd.net.        3592 IN NSEC \000.ent1.sfdcsd.net. RRSIG NSEC TY
sfdcsd.net.             3592 IN SOA dns1.p08.nsone.net. hostmaster.nsone
                                1619363158 ; serial
                                43200      ; refresh (12 hours)
                                7200       ; retry (2 hours)
                                1209600    ; expire (2 weeks)
                                3600       ; minimum (1 hour)
                                )
sfdcsd.net.             3592 IN RRSIG SOA 13 2 3600 (
                                20210712120255 20210710120255 44688 sfdc
                                m2J7Q6mk6Y8lNxXEWVNw2/cVJPIeHZMAAeYglTgy
                                mXV5hTtOpydytWFynIjdKf8YeGOpZm3zqoyLyPgM
```

3. Status of Black Lies specification

Despite the fact that Black Lies is not standardized or even formally published as a protocol specification, it seems to be gaining in popularity and deployment. At least 3 major DNS providers (Cloudflare, NS1 and Amazon Route53) have deployed it. Due to the fact that Black Lies relies on contorting existing semantics of the DNS protocol, it seems unlikely that it could be published as a "Standards Track" specification. But given deployment realities, it seems desirable to have a stable specification published for it, even if its status is Informational.

4. Implementation Status

NS1 has implemented the scheme described in this document. Example code to infer NXDOMAIN from Black Lies NODATA responses can be found here: https://github.com/shuque/blrcode

5. Acknowledgements

Jan Vcelak of NS1.

6. IANA Considerations

TBD based on DNSOP working group deliberations.

7. Security Considerations

The method proposed in this document addresses a potential security issue, namely reliably determining NXDOMAIN in Black Lies implementations.

8. References

8.1. Normative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

8.2. Informative References

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

Author's Address

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

Email: shuque@gmail.com