Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: August 22, 2021

W. Hardaker
USC/ISI
V. Dukhovni
Bloomberg, L.P.

February 18, 2021

Guidance for NSEC3 parameter settings
draft-hardaker-dnsop-nsec3-guidance-01

Abstract

NSEC3 is a DNSSEC mechanism providing proof of non-existence by promising there are no names that exist between two domainnames within a zone. Unlike its counterpart NSEC, NSEC3 avoids directly disclosing the bounding domainname pairs. This document provides guidance on setting NSEC3 parameters based on recent operational deployment experience.

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 August 22, 2021.

Table of Contents

1. Introduction

As with NSEC [RFC4035], NSEC3 [RFC5155] provides proof of non-existence that consists of signed DNS records establishing the non-existence of a given name or associated Resource Record Type (RRTYPE) in a DNSSEC [RFC4035] signed zone. In the case of NSEC3, however, the names of valid nodes in the zone are obfuscated through (possibly multiple iterations of) hashing via SHA-1. (currently only SHA-1 is in use within the Internet).

NSEC3 also provides "opt-out support", allowing for blocks of unsigned delegations to be covered by a single NSEC3 record. Opt-out blocks allow large registries to only sign as many NSEC3 records as there are signed DS or other RRsets in the zone - with opt-out, unsigned delegations don't require additional NSEC3 records. This sacrifices the tamper-resistance proof of non-existence offered by NSEC3 in order to reduce memory and CPU overheads.

NSEC3 records have a number of tunable parameters that are specified via an NSEC3PARAM record at the zone apex. These parameters are the Hash Algorithm, processing Flags, the number of hash Iterations and the Salt. Each of these has security and operational considerations that impact both zone owners and validating resolvers. This document provides some best-practice recommendations for setting the NSEC3 parameters.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Recommendation for zone publishers

The following sections describe recommendations for setting parameters for NSEC3 and NSEC3PARAM.

2.1. Algorithms

The algorithm field is not discussed by this document.

2.2. Flags

The flags field currently contains a single flag, that of the "Opt-Out" flag [RFC5155], which specifies whether or not NSEC3 records provide proof of non-existence or not. In general, NSEC3 with the Opt-Out flag enabled should only be used in large, highly dynamic zones with a small percentage of signed delegations. Operationally, this allows for less signature creations when new delegations are inserted into a zone. This is typically only necessary for extremely large registration points providing zone updates faster than real-time signing allows. Smaller zones, or large but relatively static zones, are encouraged to use a Flags value of 0 (zero) and take advantage of DNSSEC's proof-of-non-existence support.

2.3. Iterations

Generally increasing the number of iterations offers little improved protections for modern machinery. Although Section 10.3 of [RFC5155] specifies upper bounds for the number hash iterations to use, there is no published guidance on good values to select. Because hashing provides only moderate protection, as shown recently in academic studies of NSEC3 protected zones (tbd: insert ref), this document recommends using an iteration value of 0 (zero). This leaves the creating and verifying hashes with just one application of the hashing algorithm.

2.4. Salt

Salts add yet another layer of protection against offline, stored dictionary attacks by combining the value to be hashed (in our case, a DNS domainname) with a randomly generated value. This prevents

advosaries from building up and remembering a dictionary of values that can translate a hash output back to the value that it derived from.

In the case of DNS, it should be noted the hashed names placed in NSEC3 records already include the fully-qualified domain name from each zone. Thus, no single pre-computed table works to speed up dictionary attacks against multiple target zones. An attacker is required to compute a complete dictionary per zone, which is expensive in both storage and CPU time.

To protect against a dictionary being built and used for a target zone, an additional salt field can be included and changed on a regular basis, forcing a would-be attacker to repeatedly compute a new dictionary (or just do trial and error without the benefits of precomputation).

Changing a zone's salt value requires the construction of a complete new NSEC3 chain. This is true both when resigning the entire zone at once, or incrementally signing it in the background where the new salt is only activated once every name in the chain has been completed.

Most users of NSEC3 publish static salt values that never change. This provides no added security benefit (because the complete fully qualified domain name is already unique). If no rotation is planned, operators are encouraged to forgo the salt entirely by using a zero-length salt value instead (represented as a "-" in the presentation format).

3. Best-practice for zone publishers

In short, for most zones, the recommended NSEC3 parameters are as shown below:

```
; SHA-1, no opt-out, no extra iterations, empty salt:
;
bcp.example. IN NSEC3PARAM 1 0 0 -
```

For very large (e.g. 10 million plus unsigned delegations) and only sparsely signed zones, where the majority of the records are insecure delegations, use of opt-out may be justified. In such (large TLD or similar) zones the alternative parameters are:

```
; SHA-1, with opt-out, no extra iterations, empty salt:
;
example. IN NSEC3PARAM 1 1 0 -
```

4. Recommendation for validating resolvers

Because there has been a large growth of open (public) DNSSEC validating resolvers that are subject to compute resource constraints when handling requests from anonymous clients, this document recommends that validating resolvers should change their behaviour with respect to large iteration values. Validating resolvers SHOULD return a SERVFAIL when processing NSEC3 records with iterations larger than 100. Note that this significantly decreases the requirements originally specified in Section 10.3 of [RFC5155].

5. Security Considerations

This entire document discusses security considerations with various parameters selections of NSEC3 and NSEC3PARAM fields.

6. Operational Considerations

This entire document discusses operational considerations with various parameters selections of NSEC3 and NSEC3PARAM fields.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

7.2. Informative References

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Appendix A. Acknowledgments

dns-operations discussion participants

Appendix B. Github Version of this document

While this document is under development, it can be viewed, tracked, issued, pushed with PRs, ... here:

https://github.com/hardaker/draft-hardaker-dnsop-nsec3-guidance

Authors' Addresses

Wes Hardaker
USC/ISI

Email: ietf@hardakers.net

Viktor Dukhovni
Bloomberg, L.P.

Email: ietf-dane@dukhovni.org