

Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 7 November 2021

W. Hardaker
USC/ISI
V. Dukhovni
Bloomberg, L.P.
6 May 2021

Guidance for NSEC3 parameter settings
draft-hardaker-dnsop-nsec3-guidance-03

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 7 November 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

title

May 2021

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in 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 [2](#)
- [1.1.](#) Requirements notation [3](#)
- [2.](#) Recommendation for zone publishers [3](#)
- [2.1.](#) Algorithms [3](#)
- [2.2.](#) Flags [3](#)
- [2.3.](#) Iterations [3](#)
- [2.4.](#) Salt [4](#)
- [3.](#) Best-practice for zone publishers [5](#)
- [4.](#) Recommendation for validating resolvers [5](#)
- [5.](#) Security Considerations [6](#)
- [6.](#) Operational Considerations [6](#)
- [7.](#) IANA Considerations [6](#)
- [8.](#) References [6](#)
- [8.1.](#) Normative References [6](#)
- [8.2.](#) Informative References [7](#)
- [Appendix A.](#) Acknowledgments [7](#)
- [Appendix B.](#) Github Version of this document [7](#)
- Authors' Addresses [7](#)

[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. Use of the opt-out feature 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.

Internet-Draft

title

May 2021

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 NSEC3PARAM flags field currently contains no flags, but individual NSEC3 records contain the "Opt-Out" flag [[RFC5155](#)], which specifies whether or not that NSEC3 record provides 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 fewer 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

NSEC3 records are created by first hashing the input domain and then repeating that hashing algorithm a number of times based on the iterations parameter in the NSEC3PARAM and NSEC3 records. The first hash is typically sufficient to discourage zone enumeration performed by "zone walking" an NSEC or NSEC3 chain. Only determined parties with significant resources are likely to try and uncover hashed

values, regardless of the number of additional iterations performed. If an adversary really wants to expend significant CPU resources to mount an offline dictionary attack on a zone's NSEC3 chain, they'll likely be able to find most of the "guessable" names despite any level of additional hashing iterations.

Most names published in the DNS are rarely secret or unpredictable. They are published to be memorable, used and consumed by humans. They are often recorded in many other network logs such as email logs, certificate transparency logs, web page links, intrusion detection systems, malware scanners, email archives, etc. Many times a simple dictionary of commonly used domain names prefixes (www, ftp, mail, imap, login, database, etc) can be used to quickly reveal a large number of labels within a zone. Because of this, there are increasing performance costs yet diminishing returns associated with applying additional hash iterations beyond the first.

Although [Section 10.3 of \[RFC5155\]](#) specifies upper bounds for the number of hash iterations to use, there is no published guidance for zone owners about good values to select. Because hashing provides only moderate protection, as shown recently in academic studies of NSEC3 protected zones [[GPUNSEC3](#)][[ZONEENUM](#)], this document recommends that zone owners SHOULD use an iteration value of 0 (zero), indicating that only the initial hash value should be placed into a DNS zone's NSEC3 records.

TODD: discuss the authoritative overhead of needing to find the right range for new random strings coming in. Note white-lies online signing differences.

[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 adversaries 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 all zones, the recommended NSEC3 parameters are as

shown below:

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

For small zones, the use of opt-out based NSEC3 records is NOT RECOMMENDED.

For very large and sparsely signed zones, where the majority of the records are insecure delegations, opt-out MAY be used.

[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 behavior with respect to large iteration values. Validating resolvers SHOULD return an insecure response when processing NSEC3 records with iterations larger than 100. Validating resolvers MAY return SERVFAIL when processing NSEC3 records with iterations larger than 500. Note that this significantly decreases the requirements originally specified in [Section 10.3 of \[RFC5155\]](#).

Note that a validating resolver MUST still validate the signature over the NSEC3 record to ensure the iteration count was not altered since record publication (see [\[RFC5155\] section 10.3](#)).

Validating resolvers returning an insecure or SERVFAIL answer in this situation SHOULD return an Extended DNS Error (EDE) {[RFC8914](#)} EDNS0 option of value [TBD].

[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. IANA Considerations

This document requests a new allocation in the "Extended DNS Error Codes" of the "Domain Name System (DNS) Parameters" registration table with the following characteristics:

- * INFO-CODE: TBD
- * Purpose: Unsupported NSEC3 iterations value
- * Reference: this document

8. References

8.1. 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>>.

8.2. Informative References

- [GPUNSEC3] Wander, M., Schwittmann, L., Boelmann, C., and T. Weis, "GPU-Based NSEC3 Hash Breaking", DOI 10.1109/NCA.2014.27, 2014, <<https://doi.org/10.1109/NCA.2014.27>>.
- [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>>.

[ZONEENUM] Wang, Z., Xiao, L., and R. Wang, "An efficient DNSSEC zone enumeration algorithm", n.d..

[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