DNS Extensions Working Group
Internet-Draft
Intended status: Informational
Expires: January 15, 2009

R. Arends
Nominet UK
P. Koch
DENIC eG
J. Schlyter
Kirei AB
July 14, 2008

Evaluating DNSSEC Transition Mechanisms
draft-ietf-dnsext-dnssec-trans-06.txt

Status of this Memo

Abstract

This document collects and summarizes different proposals for alternative and additional strategies for authenticated denial in DNS responses, evaluates these proposals and gives a recommendation for a way forward. It is a snapshot of the DNSEXT working group discussion of June 2004.

Table of Contents

1. Introduction

This report shall document the process of dealing with the NSEC zone walking problem late in the Last Call for [RFC4033], [RFC4034], and [RFC4035] (further referred to as DNSSEC-bis, with the obsoleted [RFC2535] representing DNSSEC). It preserves some of the discussion that took place in the DNSEXT WG during the first half of June 2004 as well as some additional ideas that came up subsequently.

This is an edited excerpt of the chairs' mail to the WG:

> The working group consents on not including NSEC-alt in the DNSSEC-bis documents. The working group considers to take up "prevention of zone enumeration" as a work item.
> There may be multiple mechanisms to allow for co-existence with DNSSEC-bis. The chairs allow the working group a little over a week (up to June 12, 2004) to come to consensus on a possible modification to the document to enable gentle rollover. If that consensus cannot be reached the DNSSEC-bis documents will go out as-is.

To ease the process of getting consensus, a summary of the proposed solutions and analysis of the pros and cons were written during the weekend.

This summary includes:

> An inventory of the proposed mechanisms to make a transition to future work on authenticated denial of existence.
> List the known Pros and Cons, possibly provide new arguments, and possible security considerations of these mechanisms.
> Provide a recommendation on a way forward that is least disruptive to the DNSSEC-bis specifications as they stand and keep an open path to other methods for authenticated denial of existence.

The descriptions of the proposals in this document are coarse and do not cover every detail necessary for implementation. In any case, documentation and further study is needed before implementation and/or deployment, including those which seem to be solely operational in nature.

2. Transition Mechanisms

In the light of earlier discussions and past proposals, we have found several ways to allow for transition to future expansion of authenticated denial. We tried to illuminate the paths and pitfalls in these ways forward. Some proposals lead to a versioning of DNSSEC, where DNSSEC-bis may co-exist with a future DNSSEC-ter, other

proposals are 'clean' but may cause delay, while again others may be plain hacks.

Some paths do not introduce versioning, and might require the current DNSSEC-bis documents to be fully updated to allow for extensions to authenticated denial mechanisms. Other paths introduce versioning and do not (or minimally) require DNSSEC-bis documents to be updated, allowing DNSSEC-bis to be deployed, while future versions can be drafted independent from or partially depending on DNSSEC-bis.

2.1. Mechanisms With Need of Updating DNSSEC-bis

Mechanisms in this category demand updates to the DNSSEC-bis document set.

2.1.1. Dynamic NSEC Synthesis

This proposal assumes that NSEC RRs and the authenticating RRSIG will be generated dynamically to just cover the (non existent) query name. The owner name is (the) one preceding the name queried for, the Next Owner Name Field has the value of the Query Name Field + 1 (first successor in canonical ordering). A separate key (the normal ZSK or a separate ZSK per authoritative server) would be used for RRSIGs on NSEC RRs. This is a defense against enumeration, though it has the presumption of online signing.

2.1.1.1. Coexistence and Migration

There is no change in interpretation other than that the next owner name might or might not exist.

2.1.1.2. Limitations

This introduces an unbalanced cost between query and response generation due to dynamic generation of signatures.

2.1.1.3. Amendments to DNSSEC-bis

The current DNSSEC-bis documents might need to be updated to indicate that the next owner name might not be an existing name in the zone. This is not a real change to the spec since implementers have been warned not to synthesize negative responses with previously cached NSEC records. A specific bit to identify the dynamic signature generating key might be useful as well, to prevent it from being used to fake positive data, i.e., to limit the damage of a compromise of the online key.

2.1.1.4. Cons

Unbalanced cost may be abused for Denial of Service (DoS) attacks on the synthesizing name servers. Also, this method requires all authoritative servers to have access to a private key. While dynamic synthesis protects against enumeration, it is not really a path for versioning.

2.1.1.5. Pros

Only a minimal amendment to DNSSEC-bis is needed to allow "dangling" pointers in an NSEC RR. However, implementations are not allowed to exploit the additional knowledge that NSEC RRs provide anyway, so this amendment is more formal in nature than actually having an influence on complying implementations.

2.1.2. Add Versioning/Subtyping to Current NSEC

This proposal introduces versioning for the NSEC RR type (a.k.a. subtyping) by adding a (one octet) version field to the NSEC RDATA. Version number 0 is assigned to the current (DNSSEC-bis) meaning, making this a 'Must Be Zero' (MBZ) for the to-be-published document set.

2.1.2.1. Coexistence and Migration

Since the versioning is done inside the NSEC RR, different versions may coexist in a zone. However, depending on future methods, that may or may not be useful. Resolvers cannot ask for specific NSEC versions but may be able to indicate version support by means of a to-be-defined EDNS option bit.

2.1.2.2. Limitations

There are no technical limitations, though introducing this method will cause delay to allow testing of the (currently unknown) new NSEC interpretation.

Since the versioning and signaling is done inside the NSEC RR, future methods will likely be restricted to a single RR type for authenticated denial (as opposed to, e.g., NSEC-alt, which currently proposes three RR types).

2.1.2.3. Amendments to DNSSEC-bis

Versioning or subtyping would require a full update of the current DNSSEC-bis documents to provide for new fields in NSEC, including the need to specify client behavior in response to unknown field values.

2.1.2.4. Cons

Although this is a clear and clean path without versioning DNSSEC as a whole, it would take some time to design, gain consensus, update the current DNSSEC-bis document set, test and implement a new DNS record type for authenticated denial.

2.1.2.5. Pros

NSEC versioning does not introduce an iteration to DNSSEC while providing a clear and clean migration strategy.

2.1.3. Type Bit Map NSEC Indicator

Bits in the type-bit-map are reused or allocated to signify the interpretation of NSEC.

This proposal assumes that future extensions make use of the existing NSEC RDATA syntax, while it may need to change the interpretation of the RDATA or introduce an alternative denial mechanism, invoked by the specific type-bit-map-bits.

2.1.3.1. Coexistence and migration

Old and new NSEC meaning could coexist, depending how the signaling would be defined. The bits for NXT, KEY, SIG or other outdated RR types are available as well as those covering meta/query types or types to be specifically allocated.

2.1.3.2. Limitations

This mechanism uses an NSEC field that was not designed for that purpose. Similar methods were discussed during the Opt-In discussion and the Silly-State discussion.

2.1.3.3. Amendments to DNSSEC-bis

The specific type-bit-map-bits must be allocated and they need to be specified as 'Must Be Zero' (MBZ) when used for standard (DNSSEC-bis) interpretation. Also, behaviour of the resolver and validator must be specified in case unknown values are encountered for the MBZ field. Currently the protocol document specifies that the validator must ignore the setting of the NSEC and the RRSIG bits, while other bits are only used for the specific purpose of the type-bit-map field.

2.1.3.4. Cons

Overloading the meaning of the type-bit-map is a straightforward hack. The type-bit-map was not only not designed for this purpose, but the text in section 5.4 of [RFC4035] was put in place to explicitly prevent this usage.

2.1.3.5. Pros

No change is needed to the on-the-wire protocol as specified in the current DNSSEC-bis document set.

2.1.4. New Apex Type

This introduces a new Apex type (parallel to the zone's SOA) indicating the DNSSEC version (or authenticated denial) used in or for this zone.

2.1.4.1. Coexistence and Migration

Depending on the design of this new RR type multiple denial mechanisms may coexist in a zone. Old validators will not understand and thus ignore the new type, so interpretation of the new NSEC scheme may fail, negative responses may appear 'bogus'.

2.1.4.2. Limitations

A record of this kind is likely to carry additional feature/ versioning indications unrelated to the current question of authenticated denial.

2.1.4.3. Amendments to DNSSEC-bis

The current DNSSEC-bis documents need to be updated to indicate that the absence of this type indicates DNSSEC-bis, and that the (mere) presence of this type indicated unknown versions.

2.1.4.4. Cons

The only other 'zone' or 'apex' record is the SOA record. Adding more RRs to the zone apex bloats QTYPE ANY responses for this apex. Even though the proposal is not new, it is yet unknown how it might fulfill authenticated denial extensions. This new RR type would only provide for a generalized signaling mechanism, not the new authenticated denial scheme. Since it is likely to be general in nature, due to this generality consensus is not to be reached soon.

2.1.4.5. Pros

This approach would allow for a lot of other per zone information to be transported or signaled in band to both (slave) servers and resolvers.

2.1.5. NSEC White Lies

This proposal disables one part of NSEC (the pointer part) by means of a special target (root, apex, owner, ...), leaving intact only the ability to authenticate denial of existence of RR sets, not denial of existence of domain names (NXDOMAIN). It may be necessary to have one working NSEC to prove the absence of a wildcard.

2.1.5.1. Coexistence and Migration

The NSEC target can be specified per RR, so standard NSEC and 'white lie' NSEC can coexist in a zone. There is no need for migration because no versioning is introduced or intended.

2.1.5.2. Limitations

This proposal breaks the protocol and is applicable to certain types of zones only (no wildcard, no multi-label names, delegation only). Most of the burden is put on the resolver side and operational consequences are yet to be studied.

2.1.5.3. Amendments to DNSSEC-bis

The current DNSSEC-bis documents need to be updated to indicate that the NXDOMAIN responses may be insecure.

2.1.5.4. Cons

Strictly speaking this breaks the protocol and doesn't really satisfy the requirements for authenticated denial of existence. Security implications need to be carefully documented: search path problems (forged denial of existence may lead to wrong expansion of non-FQDNs [RFC1535]) and replay attacks to deny existence of records. In addition, this does not provide for a versioning or signalling scheme.

2.1.5.5. Pros

Solves the enumeration problem without the need of additional RR types.

2.1.6. NSEC Optional via DNSKEY Flag

A new DNSKEY Flag may be defined to declare NSEC optional per zone.

2.1.6.1. Coexistence and Migration

Current resolvers/validators will not understand the Flag bit and will have to treat negative responses as bogus. Otherwise, no migration path is needed since NSEC is simply turned off.

2.1.6.2. Limitations

NSEC can only be made completely optional at the cost of being unable to prove unsecure delegations (absence of a DS RR). An almost identical approach would just disable authenticated denial for non-existence of nodes.

2.1.6.3. Amendments to DNSSEC-bis

New DNSKEY Flag to be defined. Resolver/Validator behaviour needs to be specified in the light of absence of authenticated denial.

2.1.6.4. Cons

DNSSEC-bis less authenticated denial doesn't fully meet the requirements and breaks the DNSSEC protocol by not fully covering the threat model. Existing implementations will be confused. Operational consequences need to be studied.

2.1.6.5. Pros

Positive responses can still be validated.

2.1.7. New Answer Pseudo RR Type

A new pseudo RR type may be defined that will be dynamically created (and signed) by the responding authoritative server. The RR in the response will cover the QNAME, QCLASS and QTYPE and will authenticate both denial of existence of name (NXDOMAIN) or RRset.

2.1.7.1. Coexistence and Migration

Current resolvers/validators will not understand the pseudo RR and will thus not be able to process negative responses so testified. A signaling or solicitation method would have to be specified.

2.1.7.2. Limitations

This method can only be used with online keys and online signing capacity.

2.1.7.3. Amendments to DNSSEC-bis

Signaling method needs to be defined.

2.1.7.4. Cons

Keys have to be held and processed online with all security implications. An additional flag for those keys identifying them as online or negative answer only keys should be considered, for the same reasons given in Section 2.1.1.

2.1.7.5. Pros

Expands DNSSEC authentication to the RCODE.

2.2. Mechanisms Without Need of Updating DNSSEC-bis

2.2.1. Partial Type-code and Signal Rollover

Carefully crafted type code/signal rollover to define a new authenticated denial space that extends/replaces DNSSEC-bis authenticated denial space. This particular path is illuminated by Paul Vixie in a Message-Id <20040602070859.0F50913951@sa.vix.com> posted to <namedroppers@ops.ietf.org> 2004-06-02.

2.2.1.1. Coexistence and Migration

To protect the current resolver for future versions, a new DNSSEC-OK bit must be allocated to make clear it does or does not understand the future version. Also, a new DS type needs to be allocated to allow differentiation between a current signed delegation and a 'future' signed delegation. Also, current NSEC needs to be rolled into a new authenticated denial type.

2.2.1.2. Limitations

None.

2.2.1.3. Amendments to DNSSEC-bis

None.

2.2.1.4. Cons

It is cumbersome to carefully craft a type code roll (TCR) that 'just fits'. The DNSSEC-bis protocol has many 'borderline' cases that need special consideration. It might be easier to do a full TCR, since a few of the types and signals need upgrading anyway.

2.2.1.5. Pros

Graceful adoption of future versions of NSEC, while there are no amendments to DNSSEC-bis.

2.2.2. A Complete Type-code and Signal Rollover

A new DNSSEC type code space is defined which can exist independent of the current DNSSEC-bis type code space.

This proposal assumes that all current DNSSEC type-codes (RRSIG/ DNSKEY/NSEC/DS) and signals (DNSSEC-OK) are not used in any future versions of DNSSEC. Any future version of DNSSEC has its own types to allow for keys, signatures, authenticated denial, etcetera.

2.2.2.1. Coexistence and Migration

Both spaces can co-exist. They can be made completely orthogonal.

2.2.2.2. Limitations

None.

2.2.2.3. Amendments to DNSSEC-bis

None.

2.2.2.4. Cons

With this path we abandon the current DNSSEC-bis. Although it is easy to roll specific well-known and well-tested parts into the re-write, once deployment has started, this path is very expensive for implementers, registries, registrars and registrants as well as resolver operators and users. A TCR is not to be expected to occur frequently, so while a next generation authenticated denial may be enabled by a TCR, it is likely that that TCR will only be agreed upon if it serves a whole basket of changes or additions. A quick introduction of NSEC-ng should not be expected from this path.

2.2.2.5. Pros

No amendments/changes to current DNSSEC-bis docset needed. It is always there as last resort.

2.2.3. Unknown (New) Algorithm in DS, DNSKEY, and RRSIG

This proposal assumes that future extensions make use of the existing NSEC RDATA syntax, while they may need to change the interpretation of the RDATA or introduce an alternative denial mechanism, invoked by the specific unknown (new) signing algorithm. The different interpretation would be signaled by use of different signature algorithms in the DS RR at the parent. Consequently, the DNSKEY RR for the child zone's KSK would contain a matching algorithm field.

2.2.3.1. Coexistence and migration

Old and new NSEC RDATA interpretation or known and unknown signatures cannot coexist in a zone. While DS RRs with both new and well known algorithm designation could both exist at the parent, that would not lead to an unambiguous interpretation of the NSEC RRs in the zone. RRSIG RRs need to cover complete RRSets, so it is not possible to sign an 'old' NSEC RR with an RRSIG using an 'old' algorithm and then, at the same owner, sign another 'new' NSEC RR with an RRSIG of the 'new' algorithm type. A similar approach was subsequently standardized in [I-D.ietf-dnsext-dnssec-experiments].

2.2.3.2. Limitations

Validating resolvers agnostic of the 'new' signing algorithm (which may be a well known algorithm, but might not be recognized due to the new code) will treat the entire zone as insecure.

The algorithm number space might be split for each future version of DNSSEC. Violation of the 'modular components' concept. We use the 'validator' to protect the 'resolver' from unknown interpretations.

2.2.3.3. Amendments to DNSSEC-bis

None.

2.2.3.4. Cons

The algorithm field was not designed for this purpose. This is a straightforward hack.

2.2.3.5. Pros

No amendments/changes to current DNSSEC-bis docset needed.

2.2.4. Unknown (New) Hash Algorithm in DS

Similar to the previous method this one uses the DS RR at the parent to signal child zone properties. Here, the digest type field of the DS RR would be used to signal presence of a different (than DNSSEC-bis) authenticated denial scheme at the child.

2.2.4.1. Coexistence and migration

Old and new NSEC RDATA interpretation or known and unknown signatures can NOT coexist in a zone.

2.2.4.2. Limitations

Validating resolvers agnostic of the 'new' hashing algorithm (which may be a well known algorithm, but might not be recognized due to the new code) will treat the entire zone as insecure.

The digest type space might be split for each future version of DNSSEC. Violation of the 'modular components' concept. We use the 'validator' to protect the 'resolver' from unknown interpretations.

2.2.4.3. Amendments to DNSSEC-bis

None.

2.2.4.4. Cons

The digest type field was not designed for this purpose. This is a straightforward hack.

2.2.4.5. Pros

No amendments/changes to current DNSSEC-bis docset needed.

3. Recommendation

The authors recommend that the working group commits to and starts work on a partial TCR, allowing graceful transition towards a future version of NSEC. Meanwhile, to accomodate the need for an immediately, temporary, solution against zone-traversal, we recommend On-Demand NSEC synthesis.

This approach does not require any mandatory changes to DNSSEC-bis, does not violate the protocol and fulfills the requirements. As a side effect, it moves the cost of implementation and deployment to the users (zone owners) of this mechanism.

4. Security Considerations

This document deals with transition mechanisms for new versions of the DNS Security Extensions. The particular considerations for the methods studied are listed in the respective sections, most importantly the requirement for keeping private keys online in Section 2.1.1 and Section 2.1.7 and the full or partial abandoning of authenticated denial in Section 2.1.5 and Section 2.1.6.

5. IANA Considerations

[[Note to the RFC Editor: This section may be removed prior to publication.]]

This document does not create any new IANA registry nor does it ask for any allocation from an existing IANA registry.

6. Acknowledgements

The authors would like to thank Sam Weiler, Mark Andrews, and Stuart Schechter for their input and constructive comments.

7. References

7.1. Normative References

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

7.2. Informative References

[I-D.ietf-dnsext-dnssec-experiments]
Blacka, D., "DNSSEC Experiments", draft-ietf-dnsext-dnssec-experiments-04 (work in progress), March 2007.

[RFC1535] Gavron, E., "A Security Problem and Proposed Correction With Widely Deployed DNS Software", RFC 1535, October 1993.

[RFC2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

Authors' Addresses

Roy Arends
Nominet UK
Edmund Halley Road
Oxford OX4 4DQ
United Kingdom

Email: roy@nominet.org.uk

Peter Koch
DENIC eG
Kaiserstrasse 75-77
Frankfurt 60329
DE

Phone: +49 69 27235 0
Email: pk@DENIC.DE

Jakob Schlyter
Kirei AB
P.O. Box 53204
Goteborg SE-400 16
Sweden

Email: jakob@kirei.se
URI: http://www.kirei.se/

Full Copyright Statement

Intellectual Property