Network Working Group
Request for Comments: 4956
Category: Experimental

R. Arends
Nominet
M. Kosters
D. Blacka
VeriSign, Inc.

July 2007

DNS Security (DNSSEC) Opt-In

Status of This Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Abstract

In the DNS security (DNSSEC) extensions, delegations to unsigned subzones are cryptographically secured. Maintaining this cryptography is not always practical or necessary. This document describes an experimental "Opt-In" model that allows administrators to omit this cryptography and manage the cost of adopting DNSSEC with large zones.

Table of Contents

1. Overview

The cost to cryptographically secure delegations to unsigned zones is high for large delegation-centric zones and zones where insecure delegations will be updated rapidly. For these zones, the costs of maintaining the NextSECure (NSEC) record chain may be extremely high relative to the gain of cryptographically authenticating existence of unsecured zones.

This document describes an experimental method of eliminating the superfluous cryptography present in secure delegations to unsigned zones. Using "Opt-In", a zone administrator can choose to remove insecure delegations from the NSEC chain. This is accomplished by extending the semantics of the NSEC record by using a redundant bit in the type map.

2. Definitions and Terminology

Throughout this document, familiarity with the DNS system (RFC 1035 [1]), DNS security extensions ([4], [5], and [6], referred to in this document as "standard DNSSEC"), and DNSSEC terminology (RFC 3090 [10]) is assumed.

The following abbreviations and terms are used in this document:

RR: is used to refer to a DNS resource record.

RRset: refers to a Resource Record Set, as defined by [8]. In this document, the RRset is also defined to include the covering RRSIG records, if any exist.

signed name: refers to a DNS name that has, at minimum, a (signed) NSEC record.

unsigned name: refers to a DNS name that does not (at least) have an NSEC record.

covering NSEC record/RRset: is the NSEC record used to prove (non)existence of a particular name or RRset. This means that for a RRset or name 'N', the covering NSEC record has the name 'N', or has an owner name less than 'N' and "next" name greater than 'N'.

delegation: refers to an NS RRset with a name different from the current zone apex (non-zone-apex), signifying a delegation to a subzone.

secure delegation: refers to a signed name containing a delegation (NS RRset), and a signed DS RRset, signifying a delegation to a signed subzone.

insecure delegation: refers to a signed name containing a delegation (NS RRset), but lacking a DS RRset, signifying a delegation to an unsigned subzone.

Opt-In insecure delegation: refers to an unsigned name containing only a delegation NS RRset. The covering NSEC record uses the Opt-In methodology described in this document.

The key words "MUST, "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY, and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [2].

3. Experimental Status

This document describes an EXPERIMENTAL extension to DNSSEC. It interoperates with non-experimental DNSSEC using the technique described in [7]. This experiment is identified with the following private algorithms (using algorithm 253):

"3.optin.verisignlabs.com": is an alias for DNSSEC algorithm 3, DSA, and

"5.optin.verisignlabs.com": is an alias for DNSSEC algorithm 5, RSASHA1.

Servers wishing to sign and serve zones that utilize Opt-In MUST sign the zone with only one or more of these private algorithms and MUST NOT use any other algorithms.

Resolvers MUST NOT apply the Opt-In validation rules described in this document unless a zone is signed using one or more of these private algorithms.

This experimental protocol relaxes the restriction that validators MUST ignore the setting of the NSEC bit in the type map as specified in RFC 4035 [6] Section 5.4.

The remainder of this document assumes that the servers and resolvers involved are aware of and are involved in this experiment.

4. Protocol Additions

In DNSSEC, delegation NS RRsets are not signed, but are instead accompanied by an NSEC RRset of the same name and (possibly) a DS record. The security status of the subzone is determined by the presence or absence of the DS RRset, cryptographically proven by the NSEC record. Opt-In expands this definition by allowing insecure delegations to exist within an otherwise signed zone without the corresponding NSEC record at the delegation's owner name. These insecure delegations are proven insecure by using a covering NSEC record.

Since this represents a change of the interpretation of NSEC records, resolvers must be able to distinguish between RFC standard DNSSEC NSEC records and Opt-In NSEC records. This is accomplished by "tagging" the NSEC records that cover (or potentially cover) insecure delegation nodes. This tag is indicated by the absence of the NSEC bit in the type map. Since the NSEC bit in the type map merely indicates the existence of the record itself, this bit is redundant and safe for use as a tag.

An Opt-In tagged NSEC record does not assert the (non)existence of the delegations that it covers (except for a delegation with the same name). This allows for the addition or removal of these delegations without recalculating or resigning records in the NSEC chain. However, Opt-In tagged NSEC records do assert the (non)existence of other RRsets.

An Opt-In NSEC record MAY have the same name as an insecure delegation. In this case, the delegation is proven insecure by the lack of a DS bit in the type map, and the signed NSEC record does assert the existence of the delegation.

Zones using Opt-In MAY contain a mixture of Opt-In tagged NSEC records and standard DNSSEC NSEC records. If an NSEC record is not Opt-In, there MUST NOT be any insecure delegations (or any other records) between it and the RRsets indicated by the 'next domain name' in the NSEC RDATA. If it is Opt-In, there MUST only be insecure delegations between it and the next node indicated by the 'next domain name' in the NSEC RDATA.

In summary,

o An Opt-In NSEC type is identified by a zero-valued (or not-specified) NSEC bit in the type bit map of the NSEC record.

- A standard DNSSEC NSEC type is identified by a one-valued NSEC bit in the type bit map of the NSEC record.

and

- An Opt-In NSEC record does not assert the non-existence of a name between its owner name and "next" name, although it does assert that any name in this span MUST be an insecure delegation.

- An Opt-In NSEC record does assert the (non)existence of RRsets with the same owner name.

4.1. Server Considerations

Opt-In imposes some new requirements on authoritative DNS servers.

4.1.1. Delegations Only

This specification dictates that only insecure delegations may exist between the owner and "next" names of an Opt-In tagged NSEC record. Signing tools MUST NOT generate signed zones that violate this restriction. Servers MUST refuse to load and/or serve zones that violate this restriction. Servers also MUST reject AXFR or IXFR responses that violate this restriction.

4.1.2. Insecure Delegation Responses

When returning an Opt-In insecure delegation, the server MUST return the covering NSEC RRset in the Authority section.

In standard DNSSEC, NSEC records already must be returned along with the insecure delegation. The primary difference that this proposal introduces is that the Opt-In tagged NSEC record will have a different owner name from the delegation RRset. This may require implementations to search for the covering NSEC RRset.

4.1.3. Dynamic Update

Opt-In changes the semantics of Secure DNS Dynamic Update [9]. In particular, it introduces the need for rules that describe when to add or remove a delegation name from the NSEC chain. This document does not attempt to define these rules. Until these rules are defined, servers MUST NOT process DNS Dynamic Update requests against zones that use Opt-In NSEC records. Servers SHOULD return responses to update requests with RCODE=REFUSED.

4.2. Client Considerations

Opt-In imposes some new requirements on security-aware resolvers (caching or otherwise).

4.2.1. Delegations Only

As stated in Section 4.1 above, this specification restricts the namespace covered by Opt-In tagged NSEC records to insecure delegations only. Clients are not expected to take any special measures to enforce this restriction; instead, it forms an underlying assumption that clients may rely on.

4.2.2. Validation Process Changes

This specification does not change the resolver's resolution algorithm. However, it does change the DNSSEC validation process.

4.2.2.1. Referrals

Resolvers MUST be able to use Opt-In tagged NSEC records to cryptographically prove the validity and security status (as insecure) of a referral. Resolvers determine the security status of the referred-to zone as follows:

- In standard DNSSEC, the security status is proven by the existence or absence of a DS RRset at the same name as the delegation. The existence of the DS RRset indicates that the referred-to zone is signed. The absence of the DS RRset is proven using a verified NSEC record of the same name that does not have the DS bit set in the type map. This NSEC record MAY also be tagged as Opt-In.

- Using Opt-In, the security status is proven by the existence of a DS record (for signed) or the presence of a verified Opt-In tagged NSEC record that covers the delegation name. That is, the NSEC record does not have the NSEC bit set in the type map, and the delegation name falls between the NSEC's owner and "next" name.

Using Opt-In does not substantially change the nature of following referrals within DNSSEC. At every delegation point, the resolver will have cryptographic proof that the referred-to subzone is signed or unsigned.

4.2.2.2. Queries for DS Resource Records

Since queries for DS records are directed to the parent side of a zone cut (see [5], Section 5), negative responses to these queries may be covered by an Opt-In flagged NSEC record.

Resolvers MUST be able to use Opt-In tagged NSEC records to cryptographically prove the validity and security status of negative responses to queries for DS records. In particular, a NOERROR/NODATA (i.e., RCODE=3, but the answer section is empty) response to a DS query may be proven by an Opt-In flagged covering NSEC record, rather than an NSEC record matching the query name.

4.2.3. NSEC Record Caching

Caching resolvers MUST be able to retrieve the appropriate covering Opt-In NSEC record when returning referrals that need them. This requirement differs from standard DNSSEC in that the covering NSEC will not have the same owner name as the delegation. Some implementations may have to use new methods for finding these NSEC records.

4.2.4. Use of the AD bit

The AD bit, as defined by [3] and [6], MUST NOT be set when:

- sending a Name Error (RCODE=3) response where the covering NSEC is tagged as Opt-In.

- sending an Opt-In insecure delegation response, unless the covering (Opt-In) NSEC record's owner name equals the delegation name.

- sending a NOERROR/NODATA response when query type is DS and the covering NSEC is tagged as Opt-In, unless NSEC record's owner name matches the query name.

This rule is based on what the Opt-In NSEC record actually proves: for names that exist between the Opt-In NSEC record's owner and "next" names, the Opt-In NSEC record cannot prove the non-existence or existence of the name. As such, not all data in the response has been cryptographically verified, so the AD bit cannot be set.

5. Benefits

Using Opt-In allows administrators of large and/or changing delegation-centric zones to minimize the overhead involved in maintaining the security of the zone.

Opt-In accomplishes this by eliminating the need for NSEC records for insecure delegations. This, in a zone with a large number of delegations to unsigned subzones, can lead to substantial space savings (both in memory and on disk). Additionally, Opt-In allows for the addition or removal of insecure delegations without modifying the NSEC record chain. Zones that are frequently updating insecure delegations (e.g., Top-Level Domains (TLDs)) can avoid the substantial overhead of modifying and resigning the affected NSEC records.

6. Example

Consider the zone EXAMPLE shown below. This is a zone where all of the NSEC records are tagged as Opt-In.

Example A: Fully Opt-In Zone.

```
EXAMPLE.                   SOA    ...
EXAMPLE.                   RRSIG  SOA ...
EXAMPLE.                   NS     FIRST-SECURE.EXAMPLE.
EXAMPLE.                   RRSIG  NS ...
EXAMPLE.                   DNSKEY ...
EXAMPLE.                   RRSIG  DNSKEY ...
EXAMPLE.                   NSEC   FIRST-SECURE.EXAMPLE. (
                                  SOA NS RRSIG DNSKEY )
EXAMPLE.                   RRSIG  NSEC ...

FIRST-SECURE.EXAMPLE.      A      ...
FIRST-SECURE.EXAMPLE.      RRSIG  A ...
FIRST-SECURE.EXAMPLE.      NSEC   NOT-SECURE-2.EXAMPLE. A RRSIG
FIRST-SECURE.EXAMPLE.      RRSIG  NSEC ...

NOT-SECURE.EXAMPLE.        NS     NS.NOT-SECURE.EXAMPLE.
NS.NOT-SECURE.EXAMPLE.     A      ...

NOT-SECURE-2.EXAMPLE.      NS     NS.NOT-SECURE.EXAMPLE.
NOT-SECURE-2.EXAMPLE       NSEC   SECOND-SECURE.EXAMPLE NS RRSIG
NOT-SECURE-2.EXAMPLE       RRSIG  NSEC ...

SECOND-SECURE.EXAMPLE.     NS     NS.ELSEWHERE.
SECOND-SECURE.EXAMPLE.     DS     ...
SECOND-SECURE.EXAMPLE.     RRSIG  DS ...
SECOND-SECURE.EXAMPLE.     NSEC   EXAMPLE. NS RRSIG DNSKEY
SECOND-SECURE.EXAMPLE.     RRSIG  NSEC ...

UNSIGNED.EXAMPLE.          NS     NS.UNSIGNED.EXAMPLE.
NS.UNSIGNED.EXAMPLE.       A      ...
```

Example A.

In this example, a query for a signed RRset (e.g., "FIRST-SECURE.EXAMPLE A") or a secure delegation ("WWW.SECOND-SECURE.EXAMPLE A") will result in a standard DNSSEC response.

A query for a nonexistent RRset will result in a response that differs from standard DNSSEC by the following: the NSEC record will be tagged as Opt-In, there may be no NSEC record proving the non-existence of a matching wildcard record, and the AD bit will not be set.

A query for an insecure delegation RRset (or a referral) will return both the answer (in the Authority section) and the corresponding Opt-In NSEC record to prove that it is not secure.

Example A.1: Response to query for WWW.UNSIGNED.EXAMPLE. A

```
      RCODE=NOERROR, AD=0

      Answer Section:

      Authority Section:
      UNSIGNED.EXAMPLE.      NS     NS.UNSIGNED.EXAMPLE
      SECOND-SECURE.EXAMPLE. NSEC   EXAMPLE. NS RRSIG DS
      SECOND-SECURE.EXAMPLE. RRSIG  NSEC ...

      Additional Section:
      NS.UNSIGNED.EXAMPLE.   A      ...
```

Example A.1

In the Example A.1 zone, the EXAMPLE. node MAY use either style of NSEC record, because there are no insecure delegations that occur between it and the next node, FIRST-SECURE.EXAMPLE. In other words, Example A would still be a valid zone if the NSEC record for EXAMPLE. was changed to the following RR:

```
      EXAMPLE.               NSEC   FIRST-SECURE.EXAMPLE. (SOA NS
                                    RRSIG DNSKEY NSEC )
```

However, the other NSEC records (FIRST-SECURE.EXAMPLE. and SECOND-SECURE.EXAMPLE.) MUST be tagged as Opt-In because there are insecure delegations in the range they define. (NOT-SECURE.EXAMPLE. and UNSIGNED.EXAMPLE., respectively).

NOT-SECURE-2.EXAMPLE. is an example of an insecure delegation that is part of the NSEC chain and also covered by an Opt-In tagged NSEC record. Because NOT-SECURE-2.EXAMPLE. is a signed name, it cannot be removed from the zone without modifying and resigning the prior NSEC record. Delegations with names that fall between NOT-SECURE-2.EXAMPLE. and SECOND-SECURE.EXAMPLE. may be added or removed without resigning any NSEC records.

7. Transition Issues

Opt-In is not backwards compatible with standard DNSSEC and is considered experimental. Standard DNSSEC-compliant implementations would not recognize Opt-In tagged NSEC records as different from standard NSEC records. Because of this, standard DNSSEC implementations, if they were to validate Opt-In style responses, would reject all Opt-In insecure delegations within a zone as invalid. However, by only signing with private algorithms, standard DNSSEC implementations will treat Opt-In responses as unsigned.

It should be noted that all elements in the resolution path between (and including) the validator and the authoritative name server must be aware of the Opt-In experiment and implement the Opt-In semantics for successful validation to be possible. In particular, this includes any caching middleboxes between the validator and authoritative name server.

8. Security Considerations

Opt-In allows for unsigned names, in the form of delegations to unsigned subzones, to exist within an otherwise signed zone. All unsigned names are, by definition, insecure, and their validity or existence cannot be cryptographically proven.

In general:

- Records with unsigned names (whether or not existing) suffer from the same vulnerabilities as records in an unsigned zone. These vulnerabilities are described in more detail in [12] (note in particular Sections 2.3, "Name Games" and 2.6, "Authenticated Denial").

- Records with signed names have the same security whether or not Opt-In is used.

Note that with or without Opt-In, an insecure delegation may have its contents undetectably altered by an attacker. Because of this, the primary difference in security that Opt-In introduces is the loss of the ability to prove the existence or nonexistence of an insecure delegation within the span of an Opt-In NSEC record.

In particular, this means that a malicious entity may be able to insert or delete records with unsigned names. These records are normally NS records, but this also includes signed wildcard expansions (while the wildcard record itself is signed, its expanded name is an unsigned name), which can be undetectably removed or used to replace an existing unsigned delegation.

For example, if a resolver received the following response from the example zone above:

Example S.1: Response to query for WWW.DOES-NOT-EXIST.EXAMPLE. A

```
       RCODE=NOERROR

       Answer Section:

       Authority Section:
       DOES-NOT-EXIST.EXAMPLE. NS     NS.FORGED.
       EXAMPLE.                NSEC   FIRST-SECURE.EXAMPLE. SOA NS \
                                      RRSIG DNSKEY
       EXAMPLE.                RRSIG  NSEC ...

       Additional Section:
```

Attacker has forged a name

The resolver would have no choice but to believe that the referral to NS.FORGED. is valid. If a wildcard existed that would have been expanded to cover "WWW.DOES-NOT-EXIST.EXAMPLE.", an attacker could have undetectably removed it and replaced it with the forged delegation.

Note that being able to add a delegation is functionally equivalent to being able to add any record type: an attacker merely has to forge a delegation to the nameserver under his/her control and place whatever records are needed at the subzone apex.

While in particular cases, this issue may not present a significant security problem, in general it should not be lightly dismissed. Therefore, it is strongly RECOMMENDED that Opt-In be used sparingly. In particular, zone signing tools SHOULD NOT default to Opt-In, and MAY choose not to support Opt-In at all.

9. Acknowledgments

The contributions, suggestions, and remarks of the following persons (in alphabetic order) to this document are acknowledged:

Mats Kolkman, Edward Lewis, Ted Lindgreen, Rip Loomis, Bill Manning, Dan Massey, Scott Rose, Mike Schiraldi, Jakob Schlyter, Brian Wellington.

10. References

10.1. Normative References

[1] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Wellington, B. and O. Gudmundsson, "Redefinition of DNS Authenticated Data (AD) bit", RFC 3655, November 2003.

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

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

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

[7] Blacka, D., "DNSSEC Experiments", RFC 4955, July 2007.

10.2. Informative References

[8] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[9] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[10] Lewis, E., "DNS Security Extension Clarification on Zone Status", RFC 3090, March 2001.

[11] Conrad, D., "Indicating Resolver Support of DNSSEC", RFC 3225, December 2001.

[12] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, August 2004.

Appendix A. Implementing Opt-In Using "Views"

In many cases, it may be convenient to implement an Opt-In zone by combining two separately maintained "views" of a zone at request time. In this context, "view" refers to a particular version of a zone, not to any specific DNS implementation feature.

In this scenario, one view is the secure view, the other is the insecure (or legacy) view. The secure view consists of an entirely signed zone using Opt-In tagged NSEC records. The insecure view contains no DNSSEC information. It is helpful, although not necessary, for the secure view to be a subset (minus DNSSEC records) of the insecure view.

In addition, the only RRsets that may solely exist in the insecure view are non-zone-apex NS RRsets. That is, all non-NS RRsets (and the zone apex NS RRset) MUST be signed and in the secure view.

These two views may be combined at request time to provide a virtual, single Opt-In zone. The following algorithm is used when responding to each query:

V_A is the secure view as described above.

V_B is the insecure view as described above.

R_A is a response generated from V_A, following standard DNSSEC.

R_B is a response generated from V_B, following DNS resolution as per RFC 1035 [1].

R_C is the response generated by combining R_A with R_B, as described below.

A query is DNSSEC-aware if it either has the DO bit [11] turned on or is for a DNSSEC-specific record type.

1. If V_A is a subset of V_B and the query is not DNSSEC-aware, generate and return R_B, otherwise

2. Generate R_A.

3. If R_A's RCODE != NXDOMAIN, return R_A, otherwise

4. Generate R_B and combine it with R_A to form R_C:

   For each section (ANSWER, AUTHORITY, ADDITIONAL), copy the records from R_A into R_B, EXCEPT the AUTHORITY section SOA record, if R_B's RCODE = NOERROR.

5. Return R_C.

Authors' Addresses

Roy Arends
Nominet
Sandford Gate
Sandy Lane West
Oxford OX4 6LB
UNITED KINGDOM

Phone: +44 1865 332211
EMail: roy@nominet.org.uk

Mark Kosters
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166
US

Phone: +1 703 948 3200
EMail: mkosters@verisign.com
URI: http://www.verisignlabs.com

David Blacka
VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166
US

Phone: +1 703 948 3200
EMail: davidb@verisign.com
URI: http://www.verisignlabs.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.