DNS Security Document Roadmap
-------------------------------
<draft-srose-dnsext-dnssec-roadmap-00.txt>

Status of this Document

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Distribution of this document is unlimited. Comments regarding this document should be sent to the author.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. 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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

DNS Security (DNSSEC) technology is comprised of extensions to the Domain Name System (DNS) protocol that provide data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures. Several documents exist to describe these extensions and the implementation specific details regarding specific digital signing schemes. The interrelationship between these different documents is discussed here. A brief overview of what to
find in which document and author guidelines for what to include in new DNS Security documents, or revisions to existing documents, is described.

Table of Contents

1. Introduction ................................................. 3
2. Interrelationship of DNS Security Documents .............. 3
3. Relationship of DNS Security Documents to other DNS Documents ......................................................... 6
4. Recommended Content for new DNS Security Documents .... 6
   4.1 Security Related Resource Records ....................... 6
   4.2 Digital Signature Algorithm Implementation ............. 7
   4.3 Refinement of Security Procedures ....................... 7
   4.4 The Use of DNS Security Extensions with Other Protocols ................................................................. 8
5. Security Considerations ....................................... 8
6. Acknowledgements ............................................. 8
7. References .................................................... 9
8. Author’s Address ............................................. 10
Expiration and File Name ....................................... 10
1. Introduction

This document is intended to provide guidelines for the development of supplemental documents describing security extensions to the Domain Name System (DNS).

The main goal of the DNS Security (DNSSEC) protocol extensions is to add data authentication and integrity services to the DNS protocol. These protocol extensions should be differentiated from DNS operational security issues, which are beyond the scope of this effort. DNS Security documents fall into one or possibly more of the following sub-categories: new DNS security resource records, implementation details of specific digital signing algorithms for use in DNS Security and Secure DNS transactions. Since the goal of DNS Security extensions is to become part of the DNS protocol standard, additional documents that seek to refine a portion of the security extensions will be introduced as the specifications progress along the IETF standards track.

There is a set of basic guidelines for each sub-category of documents that explains what should be included, what should be considered a protocol extension, and what should be considered an operational issue. Currently, there are at least two documents that fall under operational security considerations that deal specifically with the DNS security extensions: The first is RFC 2541 which deals with the operational side of implementing the security extensions. The other is the CAIRN DNSSEC testbed Internet draft [CAIRN]. These documents should be considered part of the operational side of DNS, but will be addressed as a supplemental part of the DNS Security roadmap. That is not to say that these two documents are not important to securing a DNS zone, but it does not directly address the proposed DNS security extensions. Authors of documents that seek to address the operational concerns of DNS security should be aware of the structure of DNS Security documentation if they wish to include their documents in the DNSEXT Working Group in addition to the DNS Operations WG.

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]. It is also assumed the reader has some knowledge of the Domain Name System [RFC1035] and the Domain Name System Security Extensions [RFC2535].

2. Interrelationship of DNS Security Documents

The DNSSEC set of documents can be partitioned into five main groups as depicted in Figure 1. All of these documents in turn are under the larger umbrella group of DNS base protocol documents. It is
possible that some documents fall into more than one of these
categories, such as RFC 2535, and should follow the guidelines for
the all of the document groups it falls into. However, it is wise to
limit the number of "uberdocuments" that try to be everything to
everyone. The documents listed in each category are current as to
the time of writing.

```
Figure 1  DNSSEC Document Roadmap

The "DNSSEC protocol" document set refers to the document that makes
up the groundwork for adding security to the DNS protocol [RFC2535]
and updates to this document. RFC 2535 laid out the goals and expec-
tations of DNS Security and the new security related Resource Records
KEY, SIG, and NXT. Expanding from this document, related document
groups include the implementation documents of various digital
signature algorithms with DNSSEC, and documents further refining the transaction of messages. It is expected that RFC 2535 will be obseleted by one or more documents that refine the set of security extensions and DNS security transactions. Documents that seek to modify or clarify the base protocol documents should state so clearly in the introduction of the document (as well as proscribe to the IETF guidelines of RFC/Internet Draft author guidelines). Also, the portions of the specification to be modified SHOULD be synopsized in the new document for the benefit of the reader. The "DNSSEC protocol" set includes the documents [RFC2535], [CLARIFY], [AUTH], [SIZE] and their derivative documents.

The "New Security RRs" set refers to the group of documents that seek to add additional Resource Record to the set of base DNS Record types. These new records can be related to securing the DNS protocol [RFC2535] [SIG0] or using DNS security for other purposes such as storing certificates [RFC2538].

The "DS Algorithm Impl." document set refers to the group of documents that describe how a specific digital signature algorithm is implemented to fit the DNSSEC Resource Record format. Each one of these documents deals with one specific digital signature algorithm. Examples of this set include [RFC2536] [RFC2537] and [RFC2539].

The "Transactions" document set refers to the group of documents that deal with the message transaction sequence of security related DNS operations. The contents and sequence for operations such as dynamic update [RFC2137] [UPDATE] and transaction signatures [RFC2845] are described in this document category. Additional message transaction schemes to support DNSSEC operation would also fall under this group, including secret key establishment [TKEY], and verification.

The final document set, "New Security Uses", refers to documents that seek to use proposed DNS Security extensions for other security related purposes. Documents that fall in this category include the use of DNS in the distribution of certificates and individual user public keys (PGP, email, etc.).

Lastly, there is a set of documents that should be classified as "Implementation Notes". Because the DNS security extensions are still in the developmental stage, there is an audience for documents that detail the transition and implementation of the security extensions. These have more to do with the practical side of DNS operations, but can also point to places in the protocol specifications that need improvement. Documents in this set may be offspring of both the DNSEXT and/or DNSOP working groups. Currently, there is only one Internet Draft that falls under this category: The report on the CAIRN DNSSEC testbed [CAIRN]. This document was submitted
through the DNSOP working group, however the main concern of this
document in the implementation and limitations of the DNS security
extensions, hence its interest to the DNS security community.
Authors of documents that deal with the implementation and opera-
tional side of the DNSSEC specifications would be advised/encouraged
to submit their documents to the DNSEXT working group as well.

3. Relationship of DNS Security Documents to other DNS Documents

The DNS security related extensions should be considered a subset of
the DNS protocol. The DNS Security working group of the IETF
(DNSSEC) has been absorbed into the larger DNS Extensions working
group (DNSEXT). Therefore, all DNS security related documents should
be seen as a subset of the main DNS architecture documents. It is a
good idea for authors of future DNS security documents to be familiar
with the contents of these base protocol documents.

4. Recommended Content for new DNS Security Documents

Documents that seek to make additions or revisions to the DNS proto-
col to add security should follow common guidelines as to minimum
required content and structure. It is the purpose of this document
roadmap to establish criteria for content that any new DNS security
protocol specifications document SHOULD contain. This criteria
SHOULD be interpreted as a minimum set of information required/needed
in a document, any additional information regarding the specific
extension should also be included in the document. These criteria
are not officially part of the IETF guidelines regarding RFC/Internet
Drafts, but should be considered as guidance to promote uniformity to
working group documents.

Since the addition of security to the DNS protocol is now considered
A general extension to the DNS protocol, any guideline for the con-
tents of a DNS Security document could be taken as a suggestion for
the contents of any DNS extension document.

4.1 Security Related Resource Records

Documents describing a new type of DNS Security Resource Record (RR)
should contain information describing the structure and use of the
new RR type. It is a good idea to only discuss one new type in a
document, unless the set of new resource records are closely related
or a protocol extensions requires the use of more than one new record
type. Specifically: each document detailing a new Security related
RR type should include the following information:
* The format of the new RR type, both "on the wire" (bit format) and ASCII representation (for text zone files), if appropriate.

* When and in what section of a DNS query/response this new RR type is to be included.

* At which level of the DNS hierarchy this new RR type is to be considered authoritative (i.e. in a zone, in a zone’s superzone) and who is authoritative to sign the new RR.

4.2 Digital Signature Algorithm Implementations

Documents describing the implementation details of a specific digital signature algorithm such as [RFC 2536, RFC 2537] for use with DNS Security should include the following information:

* The format/encoding of the algorithm’s public key for use in a KEY Resource Record.

* The acceptable key size for use with the algorithm.

* The current known status of the algorithm (as one of REQUIRED, RECOMMENDED, or OPTIONAL).

In addition, authors are encouraged to include any necessary description of the algorithm itself, as well as any known/suspected weaknesses as an appendix to the document. This is for reference only, as the goals of the DNSEXT working group is to propose extensions to the DNS protocol, not cryptographic research.

4.3 Refinement of Security Procedures

This set of documents includes DNS protocol operations that relate to DNS Security specifically such as DNS secret key establishment [TKEY] and security extensions to pre-existing or proposed DNS operations such as dynamic update [RFC2137]. Documents that describe a new set of DNS message transactions, or seek to refine a current series of transaction that make up a DNS operation SHOULD include the following information:

* The order in which the DNS messages are sent by the operation initiator and target.

* The format of these DNS messages.

* Any required authentication mechanisms for each stage of the
operation and the required authority for that mechanism (i.e. zone, host, or some other trusted authority such as a DNS administrator or certificate authority).

4.4 The Use of DNS Security Extensions with Other Protocols

Because of the flexibility and ubiquity of the DNS, there may exist other Internet protocols and applications that could make use of, or extend, the DNS security protocols. Examples of this type of document include the use of DNS to support the Public Key Infrastructure (PKI). It is beyond the scope of this roadmap to describe the contents of this class of documents. However, if uses or extensions require the addition or modification of a DNS Resource Record type or DNS query/response transactions, then the guidelines laid out in the previous sections of this document SHOULD be adhered too.

5. Security Considerations

This document provides a roadmap and guidelines for writing DNS Security related documents. The reader should follow all the security procedures and guidelines described in the DNS Security Extensions document [RFC2535].

6. Acknowledgements

In addition to the RFCs mentioned in this document, there are also numerous Internet drafts that fall in one or more of the categories of DNS Security documents mentioned above. Depending on where (and if) these documents are on the IETF standards track, the reader may not be able to access these documents through the RFC repositories. For that reason, the version of the Internet drafts that were referenced in this document are given below:

* SIG0: D. Eastlake. "DNS Request and Transaction Signatures (SIG(0))" <draft-ietf-dnsext-sig-zero-02.txt>.
* SIGALG: R. Austein, P. Vixie. "DNS SIGALGOPT". <draft-ietf-dnsind-sigalgopt-00.txt>
* CLARIFY: E. Lewis. "DNS Security Extension Clarification on Zone Status" <draft-ietf-dnsext-zone-status-01.txt>
* CAIRN: D. Massey, T. Lehman, and E. Lewis. "DNSSEC Implementation in the CAIRN Testbed". <draft-ietf-dnsop-dnsseccairn-00.txt>
7. References


8. Authors’ Addresses

Rose