DNS Extensions
Internet-Draft
Expires: August 5, 2003

S. Rose
NIST

February 4, 2003

DNS Security Document Roadmap
draft-ietf-dnsext-dnssec-roadmap-07

Status of this Memo

Copyright Notice

Abstract

DNS Security (DNSSEC) technology is composed 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

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

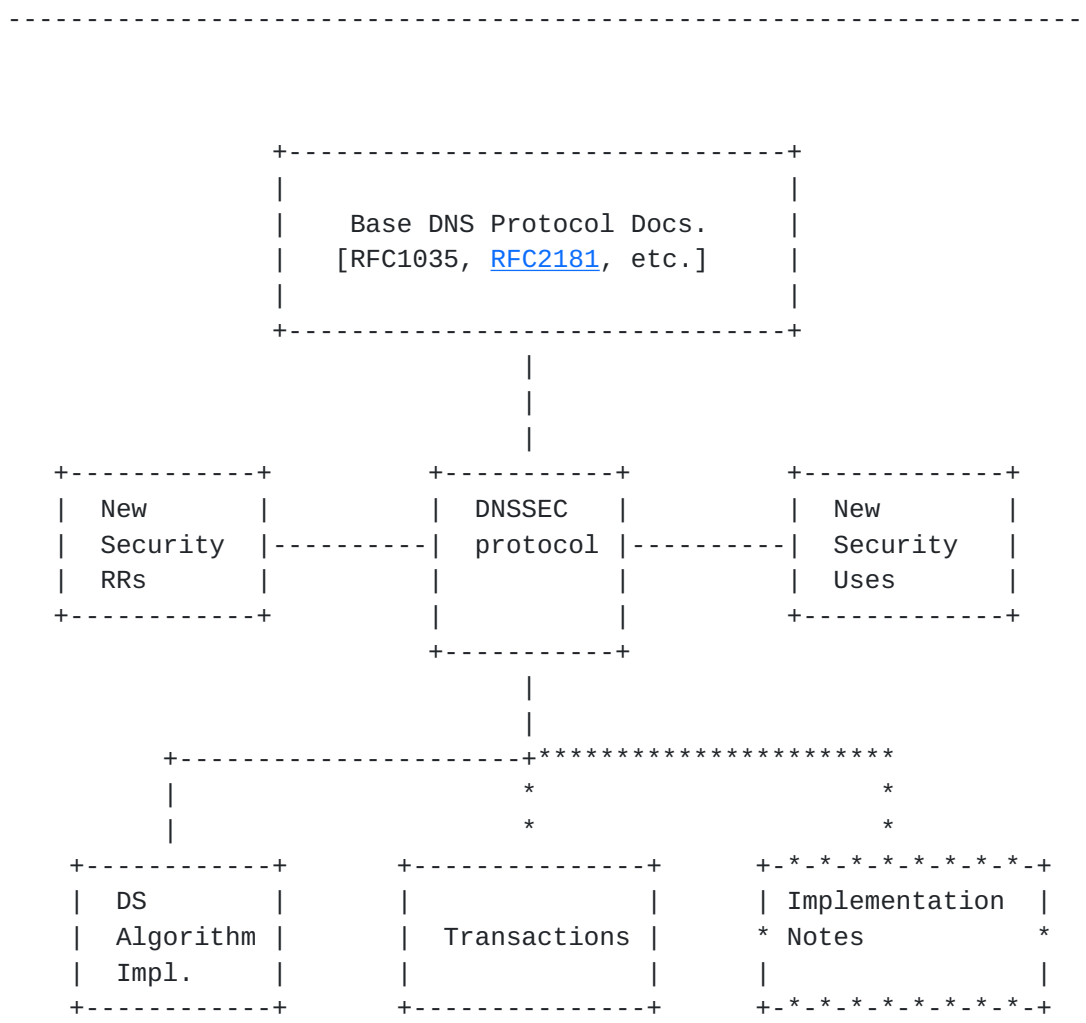
The main goal of the DNS Security (DNSSEC) extensions is to add data authentication and integrity services to the DNS protocol. These protocol extensions should be differentiated from DNS operational security issues, which are beyond the scope of this effort. DNS Security documents fall into one or possibly more of the following sub-categories: new DNS security resource records, implementation details of specific digital signing algorithms for use in DNS Security and DNS transaction authentication. 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 [6] 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 they do 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.

It is assumed the reader has some knowledge of the Domain Name System [2] and the Domain Name System Security Extensions.

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.



DNSSEC Document Roadmap

The "DNSSEC protocol" document set refers to the document that makes up the groundwork for adding security to the DNS protocol [1]and updates to this document. RFC 2535 laid out the goals and expectations of DNS Security and the new security-related Resource Records KEY, SIG, DS, and NXT [23]. 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 obsoleted by one or more documents that refine the set of security extensions [22], [23], [24]. 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 [1], [11], [12], [9], [14], [15], [21], [16], [OPTIN], [17] and their derivative documents.

The "New Security RRs" set refers to the group of documents that seek to add additional Resource Records to the set of base DNS Record types. These new records can be related to securing the DNS protocol [1], [8], or using DNS security for other purposes such as storing certificates [5]. Another related document is [26]. While not detailing a new RR type, it defines a flag bit in the existing KEY RR. This flag bit does not affect the protocol interpretation of the RR, only a possible operational difference. Therefore, this draft is place here and not with the protocol document set.

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 [4], [5], [25], [19][18] and [13].

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 [3], [11] and transaction signatures [10] are described in this document category. Additional message transaction schemes to support DNSSEC operation would also fall under this group, including secret key establishment [7], [RENEW], 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 storage and distribution of certificates and individual user public keys (PGP, e-mail, etc.) Some documents in this group may fall beyond the DNSEXT WG scope, but they are included because of their use of the security extensions. The documents in this group should not propose any changes to the DNS protocol to support other protocols; only how existing DNS security records and transactions can be used to support other protocols. Such documents include [SSH-DNS] and [IPSEC-DNS] which deals with storing SSH and IPSec keying information the DNS using new records and utilizing DNSSEC to provide authentication and integrity checking.

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. An example of this type is the report on the CAIRN DNSSEC testbed [CAIRN] This document was submitted through the DNSOP Working Group at the time of this writing, however the main concern of this document is the implementation and limitations of the DNS security extensions, hence their interest to the DNS security community. The CAIRN draft deals with the implementation of a secure DNS. Authors of documents that deal with the implementation and operational side of the DNSSEC specifications would be advised/encouraged to submit their documents to any other relevant DNS related WG meeting in the problem space.

3. Relationship of DNS Security Documents to other DNS Documents

The DNS security-related extensions should be considered a subset of the DNS protocol. 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 protocol 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. These 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 contents of a DNS Security document could be taken as a framework suggestion for the contents of any DNS extension document. The development process of the DNS security extensions could be used as a model framework for any, more general DNS extensions.

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 extension 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 [4] ,[13] (and others as new digital signatures schemes are introduced) 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 know/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 specifically relate to DNS Security, such as DNS secret key establishment [7] and security extensions to pre-existing or proposed DNS operations such as dynamic update [3]. Documents that describe a new set of DNS message transactions, or seek to refine a current series of transactions 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 IPSEC [IPSEC-DNS], SSH [SSH-DNS] 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 to.

5. Security Considerations

This document provides a roadmap and guidelines for writing DNS Security related documents. This document does not discuss the aspects of the DNS security extensions. The reader should refer to the documents outlined here for the details of the services and shortcomings of DNS security.

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. All of these documents are "Work in Progress" and are subject to change; therefore a version number is not supplied for the current revision. Some Internet Drafts are in the RFC editor's queue or nearing WG Last Call at the time of writing. These Drafts have been placed in the References section. The drafts below are still subject to agreement in the IETF.

- CAIRN: D. Massey, T. Lehman, and E. Lewis. "DNSSEC Implementation in the CAIRN Testbed". draft-ietf-dnsop-dnsseccairn-NN.txt

- OPTIN: M. Kosters. "DNSSEC Opt-in for Large Zones" draft-kosters-dnsext-dnssec-opt-in-NN.txt

- SSH-DNS: W. Griffin, J. Schlyter. "Using DNS to securely publish SSH key fingerprints" draft-ietf-secsh-dns-NN.txt

- IPSEC-DNS: M. Richardson. "A method for storing IPsec keying material in DNS". draft-richardson-ipsec-rr-NN.txt

- RENEW: Y. Kamite, M. Nakayama. "TKEY Secret Key Renewal Mode". draft-ietf-dnsext-tkey-renewal-mode-NN.txt

Normative References

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

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

[3] Eastlake, D., "Secure Domain Name System Dynamic Update", RFC 2137, April 1997.

[4] Eastlake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.

[5] Eastlake, D. and O. Gudmundsson, "Storing Certificates in the Domain Name System (DNS)", RFC 2538, March 1999.

[6] Eastlake, D., "DNS Security Operational Considerations", RFC 2541, March 1999.

[7] Eastlake, D., "Secret Key Establishment for DNS (TKEY RR)", RFC 2930, September 2000.

[8] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, September 2000.

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

[10] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

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

[12] Wellington, B., "Domain Name System Security (DNSSEC) Signing Authority", RFC 3008, April 2000.

[13] Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.

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

[15] Gudmundsson, O., "DNSSEC and IPv6 A6 aware server/resolver message size requirements", RFC 3226, December 2001.

[16] Massey, D. and S. Rose, "Limiting the Scope of the KEY Resource Record (RR)", RFC 3445, December 2002.

Informative References

[17] Austein, R. and D. Atkins, "Threat Analysis of the Domain Name System (Work in Progress)", RFC XXXX.

[18] Eastlake, R., "Storage of Diffie-Hellman Keys in the Domain Name System (DNS) (Work in Progress)", RFC XXXX.

[19] Eastlake, D. and R. Schroeppel, "Elliptic Curve KEYs in the DNS (Work in Progress)", RFC XXXX.

[20] Gundmundsson, O., "Delegation Signer Record in Parent (Work in Progress)", RFC XXXX.

[21] Wellington, B., "Redefinition of the DNS AD bit (Work in Progress)", RFC XXXX.

[22] Arends, R., Larson, M., Massey, D. and S. Rose, "DNS Security Introduction and Requirements (Work in Progress)", RFC XXXX.

[23] Arends, R., Larson, M., Massey, D. and S. Rose, "Resource Records for DNS Security Extensions (Work in Progress)", RFC XXXX.

[24] Arends, R., Larson, M., Massey, D. and S. Rose, "Protocol Modifications for the DNS Security Extensions (Work in Progress)", RFC XXXX.

[25] Kwan, S., Garg, P., Gilroy, J. and L. Esibov, "GSS Algorithm for TSIG (Work in Progress)", RFC XXXX.

[26] Kolkman, O. and J. Schlyter, "KEY RR Key-Signing-Key (KSK) Flag (Work in Progress)", RFC XXXX.

Author's Address

Scott Rose
National Institute for Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899-3460
USA

EMail: scott.rose@nist.gov

Full Copyright Statement

Acknowledgement

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