Internet Engineering Task Force
Internet-Draft
July 9, 2001

Ed Lewis
NAI Labs
Expires: January 9, 2002

The DNS SEC RR
<draft-lewis-dnsext-sec-rr-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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.

This draft expires on January 9, 2002.

Abstract

The Security Resource Record (SEC RR) is defined to hold security specific parameters of a zone. The record is stored at the apex of a zone and is used to inform resolvers of certain security aspects of a zone.

1.0 Introduction

The initial definition of DNS Security [RFC 2535] lacks a mechanism to convey any kind of security version mechanism. Such a mechanism is needed to migrate from some initial design decisions that have proven to be naive.

(Editing note: this proposal appeared on the dnssec@cafax.se mailing list in May. There has been some discussion on the need for a record like the SEC RR, but this discussion is not folded into this version. In particular, the need to convey whether "opting-in" is done or not has not been defined yet. That may be done through a security

parameters RR [SEC RR], or via another method.)

1.1 The NXT versus NO debate

The driving force for this definition is the debate concerning the authenticated denial service (commonly a signed version of NXDOMAIN, if you will). The NXT RR is defined which accomplishes authenticated denial using approach of "this is what I have, you can see the data you want is not in the range I am showing." The basic discomfort with this is the exposure of data without an explicit request. A competing proposal has been made, called the NO record.

One thought to be expressed is that the strategy employed by NXT is fine given the public nature of DNS. DNS is not intended to hold sensitive or restricted data. Although any specific piece of information is public, administrators don't want to divulge all information at once. There are two precedents for this. One is the restriction of AXFR or zone transfer requests. The other is an analogy to a company internal phone book. In the latter, asking for any specific number is acceptable, asking for the entire company's roster is not.

The NO record, defined in [draft-no] provides authenticated denial without exposing zone contents in plain text. For details of this, consult the NO document.

One of the road blocks to the adoption of NO is the inability to inform a resolver that authenticated denial provided by NO rather than NXT. The SEC RR is defined to remove this roadblock, and road blocks to other DNS Security improvements.

1.2. Statement on DNS Security and Maturity

DNS Security is just now being exposed to operational environments. It would be premature to suggest massive changes to the current definition until the real issues are defined. This proposal is being generated (actually regenerated) in response to comments on the NXT vs. NO debate. The intent is not to rush to a definition, but to collect the current needs as well as others exposed in the further development of DNS Security.

1.3 Past efforts

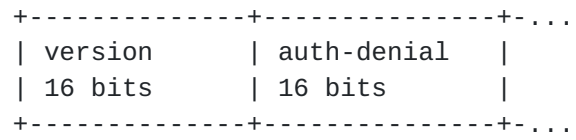
Retired drafts have defined proposals for a similar record. Most significantly, in 1999, a SEC RR was proposed to be held at the parent's side of a delegation point. The theory was that is the parent was secured, a resolver descending the tree would hear from the trusted parent about the as yet untrusted child.

There was a significant comment against the proposal, mostly because this would be a first record held at the parent-child delegation point that would be authoritative from the parent.

In this proposal, the SEC RR is again at the apex, but authoritative from the child.

2.0 The SEC RR

The SEC RR has two defined fields, but should be expanable. The defined fields are <version> and <auth-denial>. The byte format of the RDATA of the SEC RR is:



2.1 version

The Version is a 16 bit unsigned integer to indicate what version of DNS Security is employed. Version 0 indicates RFC 2535 is employed.

(Editorial note: this definition is debateable.)

2.2 auth-denial

This 16 bit number indicates the RR type value of the mechanism used for authenticated denial. A value of <NXT type> indicates NXT is used, a value of <NO type> indicates the NO is used. Special values for other options, such as opt-in [mark's draft] are also allocated (in my mind, not on paper).

2.3 ...

If there are other parameters that need to be expressed, fields can be allocated. (The entire length of the RDATA is stored in RDATALEN, so fields can just accumulate without endangering older software.)

3.0 Default values

In the abscence of an SEC RR, a resolver is to assume version 0, using the NXT RR.

4.0 Acknowledgements

Mark Kosters has asked me to revive this proposal. John Gilmore provided the objections to the previous SEC RR (1999).

5.0 IANA Considerations

The SEC RR requires a DNS type, from the pool of numbers for "normal" records, e.g., those stored in zone.

6.0 Security Considerations

One important aspect in determing the soundness of data from a security point of view is that all parameters are "as expected." This records helps the resolver to know that to expect about the server, increasing the value of performing security inspections.

7.0 References

The text of any RFC may be retrieved by a web browser by requesting the URL: ftp://ftp.isi.edu/in-notes/rfc<wxyz>.txt, where "wxyz" is the number of the RFC.

[RFC 2026] "The Internet Standards Process -- Revision 3", Bradner
[RFC 2535] "Domain Name System Security Extensions", Eastlake

The following drafts may be retrieved from a URL begining with:
    http://www.ietf.org/internet-drafts/
and followed with the file name indicated below. Note that the -dd for digit) may change over time.

[draft-no] draft-ietf-dnsext-not-existing-rr-xx.txt
[mark's draft] draft-ietf-dnsext-dnssec-opt-in-00.txt

8.0 Editor's Address

Edward Lewis
<lewis@tislabs.com>
3060 Washington Rd (Rte 97)
Glenwood, MD 21738
+1(443)259-2352

9.0 Full Copyright Statement

"AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.