Network Working Group
Request for Comments: 3130
Category: Informational

E. Lewis
NAI Labs

June 2001

Notes from the State-Of-The-Technology: DNSSEC

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

This is a memo of a DNSSEC (Domain Name System Security Extensions) status meeting.

1.0 Introduction

A meeting of groups involved in the development of the DNS Security Extensions (DNSSEC) was held in conjunction with the 49th IETF. The discussion covered the extent of current efforts, a discussion of what questions are being asked of DNSSEC, and what is needed by the IETF to progress the definition to the Draft Standard level.

DNSSEC [RFC 2535] has been under consideration for quite a few years, with RFC 2535 being the core of the most recent definition. DNSSEC is part of the charter of two working groups, DNSEXT and DNSOP. ISC's BIND v8.2 implemented part of the specification, BIND v9 represents the first full implementation. In 1999 and 2000, more than a half dozen workshops have been held to test the concepts and the earliest versions of implementations. But to date, DNSSEC is not in common use.

The current collective wisdom is that DNSSEC is 1) important, 2) a buzzword, 3) hard, 4) immature. To capture the true state of the technology and identify where work is needed, an informal gathering of groups known to be involved in DNSSEC was held in conjunction with the 49th IETF. The attendees represented NLnet Labs, The Foundation for Internet Infrastructure, RIPE NCC, ARIN, CAIRN (ISI and NAI Labs), NIST, DISA, RSSAC, Network Associates and Verisign (COM/NET/ORG TLDs).

The agenda of the meeting consisted of three items. Reports from each group on their current research goals were followed by a discussion of questions being asked of DNSSEC. Finally, with reaching Draft Standard status as a goal, what was needed to make this happen was considered.

This report is not simply a transcript of the meeting, it is a summary. Some of the information presented here was obtained in direct contact with participants after the meeting.

1.1 What does the term "DNSSEC" mean?

One of the comments made during discussions is that DNSSEC does not refer to just one monolithic technology. The term has come to refer to "toolbox" of techniques and methodologies, that when used properly can improve the integrity of the DNS. Given this observation, it can be seen that some portions of DNSSEC are evolving much more rapidly than other portions. In particular, TSIG [RFC 2845] has certainly reached a level "being deployable" for zone transfers.

The following four components are considered to be part of DNSSEC. The concept of digital signature protection of DNS traffic as described in RFC 2535 and a few support documents (such as [RFC 3008]), which is designed to protect the transfer of data on an Internet scale. The concept of protecting queries and responses through the less-scalable but more efficient TSIG mechanism [RFC 2845], which has applicability to zone transfers, DHCP registrations, and other resolver to name server traffic. Secure dynamic updates [RFC 3007], by virtue of using TSIG, can be considered to be part of DNSSEC. Finally, the definition of the CERT resource record [RFC 2538] gives DNS the ability to become a distribution mechanism for security data.

This definition of the components of DNSSEC is in no way definitive. To be honest, this is a somewhat artificial grouping. DNSSEC does not encompass all of the security practiced in DNS today, for example, the redefinition of when and how data is cached [RFC 2181], plays a big role in hardening the DNS system. The four elements of DNSSEC described in the previous paragraph are grouped together mostly because they do interrelate, but also they were developed at approximately the same time.

2.0 Group Reports

The first part of the meeting consisted of reports of goals. From this a taxonomy of efforts has been made to see if there are gaps in the work.

2.1 NLnet Labs

Efforts by NLnet Labs are directed towards yielding an understanding of the impact of DNSSEC on ccTLDs, specifically .de (Germany), .nl (The Netherlands), and .se (Sweden). Work to date has studied the problem of applying digital signatures and NXT records to a zone. The conclusion drawn is that there are no real problems regarding memory or CPU speed when signing large zones, not even for ".com." NLnet Labs has offered to work with Verisign to examine this further.

NLnet Labs is trying to define and document procedures for TLD registries, registrars and registrants to properly handle actions like zone-resigning and key-rollover at the root, TLD, and lower levels. The outcome so far is that the DNSOP Roll Over proposal seems impractical or possibly even impossible to implement at large TLDs. NLnet Labs will produce a draft on an alternative KEY+SIG handling scheme where SIGs are only kept in the zone where the corresponding zone-KEY is located. This scheme reduces the necessary actions for resigning zones from 2 levels (current zone and all children) to 1 level (current zone), and for key-rollover from 3 levels (parent, current zone and all children) to 2 levels (parent and current zone).

2.2 Verisign

Verisign’s registry operations and corporate components have been investigating what DNSSEC means to very large zones, not just from a hardware point of view, but from an institutional point of view. With the service of providing delegations already commercialized, they are attempting to define what it would take to provide a DNSSEC service. An important issue is the parent validation of each delegated zone’s keys.

2.3 The Foundation for Internet Infrastructure

The Foundation for Internet Infrastructure, an organization in Sweden, is running a project with two parts. One part is directed at the "topology" of the participants in DNSSEC, the other part of the project is directed towards general development of tools.

The study is examining the administrative issues of running DNSSEC. One issue is the possible 4-party interaction in the use of DNSSEC. The four parties are the registry, the registrar, the registrant, and the DNS operator. Of these four parties, any combination may occur within one entity, such as a registrant that operates their own DNS as part of their information technology department.

The other part of the study is looking at what happens in the resolver. Goals include DNSSEC-enabling tools such as ISAKMPd (an IPSEC key negotiation software) secure NTP4, and e-mail. Part of this effort is implemented in the sigz.net experiment, information on this exists at www.sigz.net.

2.4 RSSAC

The RSSAC (Root Server System Advisory Committee) has come to the conclusion that TSIG is worthwhile and should be deployed. There is no schedule for deployment, however.

As for the rest of DNSSEC, there is a need to better understand the impact of the new features before being introduced into production. Currently issues regarding potential testbeds are being documented. Two fundamental assumptions are that a DNSSEC testbed involving the root servers is desirable and that such a testbed would allow for long term testing. The latter assumption is based upon the need to understand how repeated zone key validations can occur at multiple independent levels of the DNS hierarchy.

2.5 CAIRN

CAIRN (Collaborative Advanced Interagency Research Network) is a DARPA-sponsored network for collaborative research. A funded activity that involves DNSSEC is FMESHD, shorthand for Fault-Tolerant Mesh of Trust in DNSSEC. The effort of this activity is to determine a means of building a resolver’s chain of trust when some of the DNS tree is unavailable or unsecured. An early deliverable of this is an extension of secure shell to retrieve keys from DNSSEC. As part of this activity, the use of DNSSEC in a non-major provider zone is being implemented and studied.

2.6 NIST

NIST is collecting performance information regarding DNSSEC. One of the fears in adopting DNSSEC is the workload it adds to existing DNS machine workload. The hopes of this effort is to quantify the fear, to see if it is real or imagined.

If time permits, there may be an effort to implement a zone integrity checking program (implemented in Java) that will look for missteps in the use of DNSSEC. Base code exists, but needs work (beyond the current baseline).

2.7 DISA

The U.S. Defense Information Systems Agency is providing funds to have DNSSEC implemented in BIND. Of particular interest is making sure that the DNSSEC specifications are correct, that BIND adheres to the specifications, and that BIND is available on the operating systems in use by the US Department of Defense. DISA expects that every line of code developed through this effort be made publicly available as part of stock BIND releases.

2.8 RIPE NCC

The RIPE NCC is looking at the impact of DNSSEC on IP-registries. The RIPE NCC is planning to coordinate and assist in the deployment of DNSSEC. Because the RIPE NCC is the Regional Internet Registry for Europe the focus will be on the deployment of DNSSEC on the reverse map tree (in-addr.arpa for IPv4).

2.9 ARIN

ARIN is investigating DNSSEC for use in signing its delegated zones under in-addr.arpa. It participated in a dnssec workshop following NANOG 20 held in Washington, DC in October, 2000. It also participated in an ipv6-dnssec workshop that followed IETF 49 in San Diego, California. Additionally, ARIN has stood up a server dedicated to testing various dns experimentation, including dnssec and carrying out limited testing.

2.10 Network Associates

NAI is pressing to get the tislabs.com zone running in accordance with DNSSEC. This is an example of a non-Internet service provider (neither an IP transit, IP address allocation, nor a domain name managing entity) making use of DNSSEC within the normal operations of the Information Technology department.

2.11 ip6.int. domain

The name servers authoritative for the ip6.int. domain are mostly upgraded to be able to support CERT records and TSIG. Once this is fully accomplished and proposals are approved, TSIG and CERT records will be used. Further DNSSEC work is unknown.

2.12 Topology Based Domain Search

Topology Based Domain Search (TBDS), is a DARPA funded activity investigating how DNS may continue to run in disconnected parts of the Internet. Topics of interest (either covered by this project, or

associated with the project) are the use of split keys, self-signed zone (keys), and multiple signing algorithms. A goal is the establishment of signed infrastructure zones, facilitating the creation of a distributed CA for activities like IPSEC and FreeSwan.

3.0 Taxonomy of efforts and What is missing

The efforts being undertaken appear to cover a broad range of work areas, from large domain registries to domain name consumers. Work has been progressing in the production of zones (signing, key management), and is starting in the use (resolver) of DNSSEC secured data.

From the discussion, there were no apparent areas lacking attention. Additional input in some areas is needed however, particularly in making use (applications and IT department) of DNSSEC.

4.0 Questions facing DNSSEC

By the 49th IETF meeting, the most pressing question on DNSSEC is "is it deployable?" From just the emphasis placed on this question, the meeting generated a list of questions and made sure that either the answer was known, or work was being done to address the question.

4.1 Is it deployable? When?

The usual answer to this has been "not now." When is always off into the future - "about a year." To get to a deployable point, a series of workshops have been held since the spring of 1999.

At this point, it is becoming clearer that longer term workshops are needed. In going through the motions of any workshop, the number of issues raised that impact the protocol’s specification is diminishing, as well as implementation issues. As such, one or two day workshops have been helping less and less in reaching deployment.

What is needed is to run longer term test configurations, possibly workshops that are help in conjunction with other events and that assume continuity. This will allow a better assessment of the issues that involve the passage of time - expirations on key validations, etc.

As was noted in section 1.1, and touched on in section 2, one component of DNSSEC, TSIG, is more advanced that the others. Use of TSIG to protect zone transfers is already matured to the "really good idea to do stage" even if other elements of DNSSEC are not. Using TSIG to protect traffic between local resolver and their "default" recursive name server still needs more work, however.

4.2 Does DNSSEC work? Is it the right approach?

Currently there is a lot of effort into making the specification as proposed work. There is some effort in assessing the specification at this point, particularly the value of the NXT records and possible replacements of it.

There seems little question on value of the KEY and SIG records. There is some research still needed on KEY validation across zone boundaries. Such work is at least scheduled.

4.3 How will client software make use of DNSSEC?

There are a number of efforts to take existing applications and have them make direct use of DNSSEC to carry out their functions. One such example is secure shell.

When or whether DNSSEC will be understood in the (using POSIX-like terms) operating systems "gethostbyname" and similar routines has not been addressed.

4.4 What are the remaining issues?

There are still a few protocol issues. The NXT resource record is designed to provide a means to authentically deny data exists. The problem is that the solution proposed may be worse than the problem, in the eyes of some. There is an alternative proposal, the NO resource record, under consideration in the DNSEXT working group. At the present time, the DNSEXT working is considering the following question: Is there a need to authentically deny existence of data, if so, which is better, NXT (being incumbent) or NO?

Another less defined issue is the mechanism for parent validation of children signatures. Although the protocol elements of this are becoming settled, the operational considerations are not, as evidenced by work mentioned in section 2. DNSSEC interactions have also been referenced in discussions over a standard registry-registrar protocol.

5.0 Progressing to Draft Standard

The IETF goal for DNSSEC is to progress the documents through the standards track [RFC 2026]. Currently, RFC 2535 is the second iteration at the Proposed standard level. There is a need to cycle through Proposed once more. Following this, the next goal is Draft.

To pass to the Draft Standard level, two main requirements must be met. There must be two or more interoperable implementations. There must also be sufficient successful operational experience.

5.1 Revision of RFC 2535 via DNSEXT

DNSEXT will soon begin a rewrite of the RFC 2535 specification (and its support documents), rolling in updates and clarifications based upon implementation and testing experience.

5.2 Operations document(s) via DNSOP

DNSOP will continue to be the forum for operations documents based upon DNSSEC activity. There is a need for the community to provide more documents to this group.

5.3 Interoperability

Demonstrating interoperability of DNSSEC, meaning the interaction of two different implementations when performing DNSSEC work, poses an issue because, to date, only BIND is seriously being fitted with DNSSEC. There are other partial implementations of DNSSEC functionality, so the potential for partial interoperability demonstrations may exist.

During the meeting, it was realized that given goals stated, a second DNSSEC implementation is needed in 18 months. Various folks in the room mentioned that they would begin see what could be done about this.

6.0 Acknowledgements

The following people attended the meeting and/or provided text for this report (in no particular order): Mark Kosters (Network Solutions), Patrik Faltstrom (Cisco), Ted Lindgreen and Miek Gieben (NLnet Labs), Jaap Akerhuis (SIDN), Olaf Kolkmann (RIPE NCC), Bill Manning and Dan Massey (ISI), Martin Fredriksson, Hakan Olsson and Jakob Schlyter (Carlstedt Research & Technology), Doug Montgomery and Scott Rose (NIST), Johan Ihren and Lars-Johan Liman (Autonomica), Brian Wellington (Nominum), Kevin Meynell (CENTR), Ed Lewis and Olafur Gudmundsson (NAI Labs).

7.0 IANA Considerations

This document does not involve assigned numbers in any way.

8.0 Security Considerations

This document, although a discussion of security enhancements to the DNS, does not itself impact security. Where security issues arise, they will be discussed in the Security Considerations of the appropriate document.

9.0 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] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

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

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

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

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

[RFC 3008] Wellington, B., "Domain Name System Security Signing Authority", November 2000.

10.0 Editor’s Address

Edward Lewis
3060 Washington Rd (Rte 97)
Glenwood, MD 21738

Phone: +1(443)259-2352
EMail: lewis@tislabs.com

11.0 Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "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.

Acknowledgement

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