RZERC00#: Recommendations Regarding Signing Root Zone Name Server Data

An Advisory from the ICANN Root Zone Evolution Review Committee (RZERC)
DD Month 2020

Preface

The Internet Corporation for Assigned Names and Numbers (ICANN) Root Zone Evolution Review Committee (RZERC) reviews proposed architectural changes to the content of the Domain Name System (DNS) root zone, the systems including both hardware and software components used in executing changes to the DNS root zone, and the mechanisms used for distribution of the DNS root zone. The RZERC was formed as a result of the Internet Assigned Numbers Authority (IANA) Stewardship Transition.

Table of Contents

1 Introduction

During RZERC's May 2020 teleconference, the Root Zone Maintainer (RZM) representative presented a proposal to sign the authoritative root zone name server data, as contained in the root-servers.net zone. The RZERC agreed that the topic falls within its charter remit since it would involve a significant change to root zone provisioning. The RZERC discussed the topic at its regular meetings and came to consensus that it needs further study. This document states the RZERC's position and recommendations on this matter.

2 Discussion

The root-servers.net zone was created in 1995 as a new way to name the root name servers. Since then, all the root name servers have been given single-letter labels in this zone, such as "k" for the name "k.root-servers.net". The primary purpose of the root-servers.net zone is to be the authoritative location for root server IP addresses.

The root zone has been signed with the Domain Name System Security Extensions (DNSSEC) since 2010. However, in the design of DNSSEC, only authoritative zone data is signed. Non-authoritative data, and glue data in particular, is not signed. In the root zone, the address records (A and AAAA) conveying the root server IP addresses are non-authoritative and thus are not signed. This means that DNSSEC can tell you whether or not one got the correct data, but not whether or not one got it from the correct server. In other words, DNSSEC doesn't authenticate sources and destinations of queries and responses, only whether or not it matches what was published by the zone operator..

Although the root zone is signed with DNSSEC, the root-servers.net zone is not. This was an intentional decision by the Root DNSSEC Design Team.[1] At the time, it was felt that signing root-servers.net was an extra complication, and not strictly necessary due to the way that DNSSEC is designed to protect DNS "leaf" data – i.e. data requested by end users.

Signed root zone name server data may be of benefit to validating recursive name servers (aka "validators"). The clear advantage being the ability to ensure that root zone queries go only to real root name server addresses. A validator could detect attempts to alter the IP addresses associated with root server identities and prevent such queries from going to a "spy-in-the-middle."

In 2017, the RSSAC published its analysis of the naming scheme for individual root servers,[2] much of which focused on having signed data for root server names and addresses. The primary recommendation of that work was that no changes should be made to the current naming scheme until more studies have been conducted.

[1] https://www.iana.org/dnssec/archive/launch-faq
[2] See RSSAC028 "Technical Analysis of the Naming Scheme Used For Individual Root Servers," https://www.icann.org/en/system/files/files/rssac-028-03aug17-en.pdf

However, signing the root zone name server data also introduces some potential problems. As demonstrated in RSSAC028, the size of a signed priming response can be significantly larger than an unsigned response, depending on the naming scheme, the server software in use, and the value of the DNSSEC_OK flag in the query. In that report, BIND version 9.10 returned a signed root-servers.net priming response exceeding 3800 bytes. In most networks this results in a UDP message broken into three fragments. RSSAC028 further showed that other software (Unbound, Knot) generate more reasonably-sized responses. It may be undesirable to rely on working fragmentation reassembly for priming queries. A group of DNS software and service providers have agreed to lower the default ENS0 UDP buffer size in their products and services to 1232 bytes.[3] This could have an impact on the ability of recursive name servers to receive a full priming response over only UDP.

Another aspect worth considering is how recursive name servers respond to bogus priming responses. In other words, do they actually check signatures and discard data from responses that cannot be validated?

3 Recommendations

Recommendation 1: The RZERC recommends that ICANN Org conduct the further studies called for in Recommendation 2 of RSSAC028 and focus on these aspects of the research:

A. Revisit the options and consequences of having signed root zone name server data.
B. Understand and document the behavior of authoritative DNS software currently in use by root server operators with respect to a signed priming response. This should include, but not necessarily be limited to, the size of a signed priming response. Would this result in a lot of UDP fragmentation? Should root server operators expect to see a significant increase in TCP traffic?
C. Understand and document the behavior of recursive name servers with respect to validating signed priming responses. Do they validate and detect incorrect data? What fraction of priming queries today have the DO bit set?

Recommendation 2: The RZERC recommends that ICANN Org Further explore the cost / benefit tradeoffs and risks of signed root zone name server data. Do the risks of redirected query traffic outweigh the risks of increased operational complexity?

~~**Recommendation 3: The RZERC recommends efforts be created to foster architectural discussions regarding the intentional design in DNSSEC whereby delegation data is not signed. Is this more important at the root? Should this be considered to apply more widely to all zones?¶**~~

[3] https://dnsflagday.net/2020/

4 Disclosures, Acknowledgements, Statements of Interest, Dissents and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the RZERC process. The Disclosure section lists the entity or entities that recommended RZERC to consider the matter per RZERC operational procedures, as well as any disclosures that RZERC members feel necessary to state in the interests of transparency. The Acknowledgments section lists the RZERC members, outside experts, and ICANN staff who authored or edited directly to this particular document or who provided reviews. The Statements of Interest section points to the biographies of all RZERC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals section, this document has the full consensus approval of all of the members of RZERC, as specified in its operational procedure.[4]

4.1 Disclosures

The RZM representative brought this proposal to the RZERC during its May 2020 teleconference.

4.2 Acknowledgements

The committee wishes to thank the following RZERC members and staff for their time, contributions, and review in producing this report.

RZERC Members:
Geoff Huston (SSAC)
Brad Verd (outgoing RSSAC representative)
Daniel Migault (incoming RSSAC representative)
Carlos Martinez (ASO)
Jim Reid (outgoing IETF representative)
Tim April (incoming IETF presentative)
Howard Eland (GNSO RySG)
Peter Koch (ccNSO)
Duane Wessels (Root Zone Maintainer)
Kaveh Ranjbar (ICANN Board)
Kim Davies (PTI)

Staff:
Danielle Rutherford (editor)
Steve Sheng

[4] See https://www.icann.org/iana_rzerc_docs/255-rzerc000v1-operational-procedure-v-final

4.3 Statements of Interest

RZERC member biographical information and Statement of Interest are available at: https://www.icann.org/rzerc-membership

4.4 Dissents and Withdrawals

There were no dissents or withdrawals.