RZERC003: Adding Zone Data Protections to the Root Zone

An Advisory from the ICANN Root Zone Evolution Review Committee (RZERC)
12 February 2021

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 add data integrity protections to the root zone using the Message Digests for DNS Zones (aka "ZONEMD") protocol, which has recently been published as RFC 8976 by the Internet Engineering Task Force (IETF). The RZERC agreed that the proposal falls within its charter remit since it involves adding new data to the root zone, in the form of the new ZONEMD record type. This document states the RZERC's position and recommendations on the ZONEMD proposal.

2 Discussion

The mechanisms of promulgating the contents of the root zone to various DNS resolvers has moved beyond just conventional DNS query and response means and now includes mechanisms that transfer the entire root zone contents to other resolvers that can then serve this zone. While zone signing and DNSSEC validation can allow individual responses to be verified, the question as to how to verify that the entire root zone content that has been transferred matches the current, originally published root zone is not well addressed by these DNSSEC validation mechanisms.

Traditionally in the DNS, zone data is transferred between name servers using the "DNS Zone Transfer Protocol," also known colloquially as AXFR. This is the standard technique for delivering zone data from primary servers to secondary servers. In the root server system, AXFR is used to transfer the root zone from the root zone maintainer (RZM) to the root server operators (RSOs).

The AXFR protocol alone provides relatively little to ensure data integrity. For this reason, the root server system uses "Secret Key Transaction Authentication," or TSIG, for zone transfers from the RZM. A TSIG key is simply a pre-shared secret. Its use in a zone transfer provides authentication, as well as data integrity checks. However, the protections afforded by TSIG are ephemeral, lasting only as long as the connection over which the data is transferred.

Since the root zone is signed with DNS Security Extensions (DNSSEC), one might expect that those signatures already provide sufficient data integrity. DNSSEC has been primarily designed to protect consumers of DNS responses (i.e., recursive and stub name servers), not entire zones as consumed by authoritative name servers.[1] For example, in the root zone, none of the delegation name server (NS) records, nor their corresponding address (A and AAAA) glue records, are signed. Also, DNSSEC protection of data only extends to end entities who use resolution mechanisms that perform DNSSEC validation.

Prior to the use of DNSSEC, it was important that recursive resolver queries only be sent to, and responses received from, the officially designated name servers for a given zone. DNS clients implicitly trusted those servers to provide authentic, unmodified answers. With the advent of DNSSEC, the source of data matters less since modification of resource records can be detected by DNSSEC validating resolvers. This, in turn, made it more feasible for recursive operators to consider downloading and serving root zone data locally.[2] Open source DNS products such as

[1] See RFC 4033: DNS Security Introduction and Requirements, Section 12, https://tools.ietf.org/html/rfc4033
[2] See RFC 8806: Running a Root Server Local to a Resolver, https://tools.ietf.org/html/rfc8806

BIND, Unbound, and Knot resolver all have the ability to download and use root zone data received from another DNS server or Uniform Resource Locator (URL). However, in a way, this creates possibilities for zone content corruption to be undetected. As locally-served zone data becomes more commonplace, a reliable technique for verifying the entirety of zone content becomes increasingly important.

A proposal for such a technique, titled Message Digests for DNS Zones, has recently been published as a proposed standard through the IETF's RFC process.[3] This protocol embeds a cryptographic digest of zone data into the zone itself, with a new ZONEMD Resource Record (RR) type. Deploying this for the root zone would necessarily require adding a ZONEMD record to the root zone. The digest value would be calculated by the RZM and included in each new version of the published root zone.

3 Impacted Parties

This section describes the impacts of this change to parties involved in root server provisioning and resolution.

Root Zone Maintainer: As publisher of the root zone, the RZM will be responsible for correctly calculating a zone digest and including a ZONEMD record in the root zone.

Internet Assigned Numbers Authority (IANA): The addition of ZONEMD to the root zone does not impose any operational requirements on IANA. In the recommendations below, IANA and the RZM will work together to develop a deployment plan.

Root Server Operators: The RSOs will need to ensure that their systems are able to accept a zone that includes the new ZONEMD resource record type. They are encouraged, but not required, to verify zone data using the zone digest technique.

Recursive Resolver Operators: In general, recursive operators are not impacted by the addition of the ZONEMD record to the root zone. Operators of recursive resolvers that are configured to serve root zone data locally are encouraged to enable ZONEMD verification when supported by their chosen software.

End Users: The addition of ZONEMD to the root zone does not impact end users of applications that issue DNS queries.

4 Recommendations

The RZERC believes that ZONEMD will be a reliable technique for verifying the root zone content. As such the RZERC supports deploying ZONEMD in the root zone, and asks the ICANN Board to organize the necessary work outlined in the following recommendations:

[3] See Message Digest for DNS Zones, https://www.rfc-editor.org/info/rfc8976

Recommendation 1: The root zone maintainer and root server operators should verify and confirm that the addition of a ZONEMD resource record will in no way negatively impact the distribution of root zone data within the RSS.

Recommendation 2: The DNS and Internet community should be made aware of plans to use ZONEMD in the root zone, and be given an opportunity to offer feedback. This may include technical presentations at meetings hosted by ICANN, the DNS Operations Analysis and Research Center (DNS-OARC), the North American Network Operators' Group (NANOG), the Réseaux IP Européens (RIPE), etc.

Recommendation 3: Developers of name server software are encouraged to implement ZONEMD and consider enabling it by default when the software is configured to locally serve root zone data.

Recommendation 4: Public Technical Identifiers (PTI) and the RZM should jointly develop a plan for deploying ZONEMD in the root zone, and make this plan available for review by RZERC.

5 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]

5.1 Disclosures

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

The RZM representative is a co-author of RFC 8976.

5.2 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:

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

Danielle Rutherford (editor)
Steve Sheng

5.3 Statements of Interest

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

5.4 Dissents and Withdrawals

There were no dissents or withdrawals.