ICANN’s Root Name Service Strategy and Implementation

ICANN Office of the Chief Technology Officer

OCTO-016v2
27 June 2022

TABLE OF CONTENTS

This document supports ICANN's strategic goal to improve the shared responsibility for upholding the security and stability of the Domain Name System (DNS) by strengthening DNS coordination in partnership with relevant stakeholders. It is part of ICANN's strategic objective to strengthen the security of the DNS and the DNS root server system (RSS).

This document is part of ICANN's Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This revision contains suggestions from many people who read OCTO-016v1. ICANN greatly appreciates the reviews sent to us.

Executive Summary

This document provides a high-level overview of the Internet Corporation for Assigned Names and Numbers (ICANN) organization's strategy and implementation plans for the ICANN Managed Root Server (IMRS). The strategy has two primary goals:

- Supporting the Internet community by improving access to the root service in diverse locations and
- Protecting availability of the root service provided by IMRS during attack.

This document is a significantly revised, second public version of ICANN's strategy and implementation plan. It reflects input received from the ICANN community on the first version of this strategy via public comment.

1. Introduction

"Root name service" is the service that responds to queries for the root of the global DNS. The root name service is provided primarily by the operators of the root server system (RSS); these operators are identified by the Internet Protocol (IP) addresses found in the root zone maintained by ICANN as part of the Internet Assigned Numbers Authority (IANA) naming function. The root name service provided by twelve independent organizations known as the root server operators (RSOs) has successfully handled increasing volumes of queries as the Internet has grown. These queries mostly originate through the millions of recursive resolvers that are operated by Internet Service Providers (ISPs), enterprise network operators, and other organizations.

Although root name service has been available without any user-noticeable disruption since the inception of the DNS, and the RSS is currently well provisioned to cope with the ongoing growth of the Internet, over the long term, risks to the availability of root name service are a growing concern due to the continued increase in denial-of-service capacity. For example, Netscout has observed an increase of 20% year-over-year in denial-of-service attacks (see Issue 6: Findings from 2H 2020 of the Netscout Threat Intelligence Report). In addition, when considering the security and stability of the root of the DNS, the integrity of the data provided in response to root queries, as well as the privacy of root service requests and responses, become areas of increased interest.

The strategy presented in this paper aims to help mitigate the risks identified by the ICANN Board as potentially significant to the secure and stable operation of those parts of the DNS that are within ICANN's remit and capability to address. These risks are primarily attacks on the availability of root service.

This document first discusses ICANN's root name service strategy and goals at a high level, then introduces the risks to root name service as identified by the ICANN Board. A discussion of the mitigations of the identified risks follows. Next, a high-level plan for implementation of the strategy will be provided, with a discussion of the implications of that implementation. Finally, conclusions will be provided.

1.1 ICANN’s Roles

ICANN has historically played four separate roles with respect to the RSS:

- Operates as one of the twelve RSOs.
- Supports the RSS in the ICANN community.
- Promotes the security of the contents of the DNS root zone.
- Promotes increased privacy of DNS requests to the RSS.

The first role, ICANN as an RSO, is performed by the Security and Network Engineering (SaNE) group of ICANN org’s Engineering and Information Technology function. The service is called “IMRS” and was also colloquially known as “L-root”.

The second role comes from ICANN’s mission as provided in its bylaws: “[ICANN] Facilitates the coordination of the operation and evolution of the DNS root name server system.” This includes support for the activities of the Root Server System Advisory Committee (RSSAC) and the RSSAC Caucus.

The third role is exemplified by ICANN’s signing of the DNS root zone with DNSSEC in 2010 and its maintenance of the integrity of the key signing key (KSK) since then. ICANN also promotes the use of DNSSEC validation to the operators’ recursive resolvers. To fulfill its fourth role, ICANN also promotes the use of privacy-enhancing technologies such as hyperlocal (also described in OCTO-027), aggressive NSEC, and QNAME minimization to those same operators.

The first role is entirely independent of the other three roles. The purpose of this strategy document is to provide the overarching framework under which ICANN org staff undertake the first role described above through the operation of IMRS.

2 Strategy and Goals

ICANN’s overarching strategy for root name service is driven by ICANN’s mission as defined by the ICANN community and described in Article 1, section 1.1 of ICANN’s Bylaws, namely to “ensure the stable and secure operation of the Internet's unique identifier systems.” Because root name service is critical to the operation of the Internet’s unique identifier system, strategically, ICANN will work with the community to identify risks that threaten root name service stability and security, then devise and implement mitigations for those risks where feasible and within ICANN’s limited technical remit and resources.

Over the long term, this strategy aims to reduce or eliminate the various risks associated with root name service. Because ICANN org is merely one player in the larger root name service ecosystem (ICANN org is just one of the twelve root server operators), a key component of this strategy will be to leverage the ICANN community and other bodies, particularly those within the DNS technical sphere. In order to ensure mitigations are having the desired effect, this strategy must also take into consideration the monitoring of various aspects of root server system behaviors in general and the operation of the IMRS in particular.

At a high level, the goals of ICANN’s root name service strategy are to use the IMRS to mitigate, as much as feasible and within ICANN’s limited technical remit, the risks associated from attacks aiming to disrupt root name service. Because ICANN’s resources are limited, it is also a goal to ensure any mitigations of the risks identified are cost-effective, sustainable, and implemented in an open, transparent, and accountable way.

3 Risks of Attack on the Root Name Service

Today, attacks against individual root server identities, either accidental or malicious, are relatively common and typically easily mitigated. Attacks on the RSS as a whole, some of which are described in Threats to the Root Server System, a report published by the RSOs in August 2019, are quite rare and have been unsuccessful to date. For example, unsuccessful attacks against the RSS as a whole occurred in 2002, 2007, and 2015, and Anonymous threatened but did not execute an attack, "Operation Global Blackout," in 2012. While these attacks did not result in noticeable impact to end users, it is safe to assume attacks will occur in the future.

Because the DNS namespace is hierarchical, domain name lookups begin at the root and traverse the domain name tree until the name is resolved or an error message is returned. While caching of information from previous lookups improves name service scalability, performance, and resiliency, an attack that negatively impacts the availability of root name service as a whole would eventually impact name resolution for all names. If such an attack were maintained for sufficient time for cached entries of the root to expire, name resolution would fail for all devices, rendering Internet use by most end users impossible.

Root name service provided by the RSS as implemented today is provisioned with vastly more resources than are needed in day-to-day service. It has 13 root server identities deployed via anycast routing on many hundreds of servers, some of which making use of cloud services that have demonstrated ability to withstand massive denial-of-service (DoS) attacks. This makes the chances of a successful DoS attack against root service as a whole exceedingly unlikely for the foreseeable future.

However, trade press reports and academic research have shown the trend in DoS attack capacity has been increasing, perhaps even in an exponential fashion. Evidence suggests this attack capacity growth is fueled by the proliferation of vulnerable devices, particularly end user or "Internet of things" devices, connected to the Internet that are compromised and subsequently used to implement attacks of various kinds. As these vulnerable devices are connected to the Internet with non-trivial and increasing bandwidth, attack capacity will logically continue to grow.

From an attacker's perspective, the cost of obtaining attack capacity does not need to take into account purchasing machines and bandwidth nor maintaining those machines or network capacity for any length of time because attackers would be making use of existing compromised devices. On the other hand, defenders must typically pay for DoS mitigation services and/or the over-provisioning of their capacity to protect against any attack and be able to deploy those protections at any time. This suggests that the aggregate cost and effort to defend against massive DoS attacks will, at some point, outpace the cost and effort to mount those attacks.

To be clear, it is highly likely the current and near-term risk to the availability of root service is minimal. To date, the RSS has never experienced end user noticeable disruption in service, and the independent RSOs have upgraded their services repeatedly over the years. However, the increase in attack capacity, the fact that cost-of-attack capacity is negligible to the attacker (the RSOs shoulder the cost of defending against attacks themselves), and the potential global impact of root name service unavailability, all point to the fact that longer-term risks should, if possible, be mitigated.

3.1 Risk Mitigations

Because the RSS is implemented by twelve independent organizations, ICANN org can only directly work to ensure the secure and stable operation of root service provided by IMRS, while informally coordinating with the other RSOs about their operations. As such, the risks targeted by this strategy are those related to the security and stability of the operation of IMRS.

The traditional approach to mitigating root name service availability risk has been to massively over-provision that service, both by increasing the CPU, memory, bandwidth, etc., used by the servers providing root name service (i.e., “growing vertically”) as well as by making use of anycast routing to deploy more servers (i.e., “growing horizontally”). This mitigation strategy has allowed the RSS to scale sufficiently to ensure root name service has remained uninterrupted in the face of numerous DoS attacks. IMRS actively uses both vertical and horizontal growth strategies.

The “vertical growth” mitigation implies expanding capacity of root name service by obtaining faster and bigger machines to act as servers, larger pipes, and associated hardware such as routers, and related infrastructure to allow a single machine or set of machines in a single location to handle the additional load.

The “horizontal growth” mitigation implies deploying more, potentially smaller and cheaper servers, on limited bandwidth pipes. However, while deploying anycast instances can be effective in ensuring at least some root name service clients for a particular RSO get responses, it is not ideal. The deployment of instances addresses the denial-of-service risk by increasing the coverage of instances throughout the Internet so that the attack traffic affects a smaller number of instances. The costs of such deployment include the cost of the machines, bandwidth, power, cooling, and so on.

In order to mitigate any risk, it is necessary to understand as well as possible the environment in which that risk may occur. Risks involving root name service are no exception. As such, a key component of mitigation of any risk associated with root name service is observation of that service and the monitoring of its behavior. In this context, observation and monitoring is aimed at understanding the “health” of root name service operation and its infrastructure as implemented by IMRS.

4 Implementation Plan

Based on the root name service risks discussed earlier, the implementation plan for the mitigations is multi-faceted, requiring efforts on the part of ICANN org in its role as the operator of the IMRS.

4.1 Vertical Scaling

In order to scale IMRS vertically, ICANN org will deploy additional multi-server clusters of instances. Each of these clusters represent significant name resolving capacity, both in terms of CPU as well as network bandwidth. An IMRS cluster is completely managed, controlled, and supervised by ICANN.

Today, IMRS has four clusters: one in Europe, two in North America, and one in Asia/Australia/Pacific. Plans are currently underway to augment these clusters with additional clusters in Africa, Asia/Australia/Pacific, and Europe.

4.2 Horizontal Scaling

In contrast to vertically scaling, in which capacity is added to single points in the IMRS infrastructure, horizontal scaling means adding additional instances in network topologically separate locations. The primary way to achieve this scaling is to make new IMRS single instances available at a low initial cost to organizations that have good connectivity relative to local standards even in places with limited connectivity that can be expected to be good long-term stewards of the instances. ICANN org focuses primarily on ISP organizations, because they are located closer to recursive resolvers used by end users, and often have good connections with other local ISPs. Note that non-ISPs are eligible even though they are not the primary focus of ICANN.

Because of the way the Internet's routing system works, "location" typically refers to Internet topology, not geographic location. A resolver in a particular autonomous system can provide a measurable number of hops from various root servers. IMRS instances are located in autonomous systems of many sizes and types. This does not preclude instances that are chosen for their geographic location. There may be reasons why placing IMRS singles in particular geographic areas makes sense; however, care is taken when selecting these areas to ensure such instances are not overly redundant.

5 Conclusion

ICANN's goals of greater availability of root service and of reducing the effects of attacks on the root system will continue to be important, given the importance of the DNS and the role that the RSS plays within it. Because ICANN is committed through its Bylaws to ensure the security, stability, and resilience of the DNS, these strategies are necessary as the value of, and risks to, the root system continue to evolve. ICANN will review this strategy as new information about the root service appears.