Threat Mitigation for the Root Server System

Root Server Operators
August 2019

Introduction

The Domain Name System (DNS) Root Server System (RSS) is a critical piece of Internet infrastructure. Almost all services on the Internet rely on the ability to resolve names and addresses in the globally-unique DNS namespace. The RSS is the first step in that resolution process and its security can affect all users of the Internet. The organizations that comprise the Root Server Operators (RSO) group recognize the importance of security and its role in supporting the Internet. In this document, we outline security risks to the RSS and general methods used for mitigation. Availability and data integrity of the root zone are currently the primary concerns of the Root Server System. Confidentiality is a secondary concern that is being addressed elsewhere (for example, in the IETF dprive working group). RSOs recognize that RSSAC001 is the de facto document on service accuracy, availability, capability, operational security and diversity of implementation. The diversity of RSOs within the RSS allow RSOs to independently employ their own mitigation strategies to lessen the threat of various attacks. RSOs may decide to share their strategy with the Root Ops community for other RSOs to test and leverage such implementations.

Threats to the Root Server System

In the following sections, we outline threats to the RSS and mitigation efforts to minimize their risk.

Denial of Service (DoS) attacks on Network Bandwidth

Recent denial of service attacks have become even more capable of saturating network bandwidth to systems and will only continue to grow. A sophisticated, global DoS attack could easily saturate any system on the Internet. The bandwidth available at the entirety of the RSS is significant, but not immune to DoS attacks. The RSS mitigation strategy is based on deploying hundreds of instances of root servers, across many different ISPs, around the world. The RSS is heavily anycasted and most operators have tens or hundreds of upstream providers and private peers. This helps to "localize" attacks and limit their effects close to the sources of traffic. It also enables operators or ISPs to track down sources of rogue traffic and engineer flows in an attempt to minimize the impact to the Internet at large (black-holing). Such measures mean that a root server does not need to handle the full bandwidth of an attack. However, mitigations can result in partial loss of legitimate traffic, at least regionally.

DoS attacks on CPU/memory consumption

DoS attacks against the CPU or memory utilization of individual root server hosts pose a threat as well. While many root server instances are "hefty" machines with plenty of CPU and memory resources available, they are not immune to attack. The replication of the RSS among multiple operators and thousands of machines reduces this threat significantly, with impact of any such attack likely being localized to particular region due to the widespread use of Anycast by the RSOs. Health checks and system monitoring by RSOs allow for quick detection of CPU and memory DoS attacks, and actions (sometimes automatic) can be taken to filter offending traffic in a similar fashion to bandwidth attacks or re-initialize processes to reduce CPU or memory exhaustion.

Protocol and Security Enhancements

As the Internet evolves, so do its protocols and security threats. Emerging changes and extensions to the DNS protocol increase complexity and processing requirements if implemented in the Root Server System. Security extensions such as DNS-over-HTTP (DoH) and DNS-over-TLS (DoT) would shift RSS traffic towards TCP with additional overhead for cryptographic operations and protocol parsing. The increased resource requirements to support such protocol enhancements will have a negative impact on the current RSS infrastructure. Studies are under way to assess the impact of known protocol changes and RSOs will carefully deliberate on which protocol extensions to support as well as use this information to help them plan for hardware and network upgrades. Some RSOs are sponsoring development of core DNS software to optimize resource usage as well as filtering of invalid or corrupt traffic in a more efficient manner.

Data Integrity

DNS data integrity is sufficiently handled with the deployment of DNSSEC (RFC4033-4035, RFC4509) in the root zone. The Root Zone Administrator and Root Zone Maintainer (RZM) are jointly responsible for its key management. Although DNSSEC validation deployment within the Internet is incomplete, it is expected that data integrity breaches would be detected by validating resolvers, answers with incorrect signatures would be thrown away, and such activity would be reported publicly as a significant concern. We continue to promote DNSSEC validation and proper trust anchor maintenance as the solution to this particular threat. The RSOs agree that the Internet Assigned Numbers Authority (IANA) is the only true source of the root zone information and cryptographic authentication and integrity checks are performed on all zone updates and transfers. Validation measurements are performed among operators to assure that the correct zone serial number is being served. The integrity of zone transfers among Root Servers is protected by DNS Transaction Signatures (TSIG) with regular key rotation.

DNSKEY Compromise

We believe that the DNSKEY protection practices instituted by IANA and the RZM are of sufficient quality that a private key compromise of the root zone DNSKEYs is sufficiently unlikely. The root zone operators will actively engage in the upcoming expected discussions surrounding the future DNSKEY rolls and plans to ensure our faith in the operational handling of the DNSKEY material remains justified. Details of the policies and procedures for maintenance of the Root Zone keying material can be found at: https://www.iana.org/domains/root.

Operator Loss/Compromise

The loss of a single RSO is discussed in RSSAC021, and the root server operators agree with the assessments therein. Specifically, we believe that the current set of identifiers significantly over-provisions the need to ensure DNS resolvers are able to contact at least one responding DNS Root Server. We consider the threat of an individual operator being "compromised" as the failure of the organization to follow the principles set forth in RSSAC037. These principles include operating with integrity and ethos, remaining neutral and impartial, and collaboration and engagement of the stakeholder community. Detection of a compromised RSO is done through automated Internet measurements (for data integrity) and through the open processes of ICANN. RSSAC037 proposes a governance model for RSOs that will allow RSOs to be removed or added. When this governance model is finalized and implemented, it will be the mechanism to handle a potentially compromised operator.

Software and System compromise

The individual root server systems, and therefore the entire RSS, is vulnerable to bugs and security threats to the name server software as well as to the Operating Systems (OS) on which they run. While most RSOs use a small set of well-known, trusted server implementations, there is still the possibility of bugs that can threaten security. To this end, operators individually choose which implementation(s) they run, and the entire RSS represents several different implementations in use. Diversity of server software limits the threat of software bugs to the RSS. The same goes for the OS on which the servers run. Each operator can choose their own baseline OS and can run different OSes on different instances. Best Common Practices for securing an OS are implemented on all RSS instances and systems are generally dedicated to operating as root servers. Health checks and systems status are closely monitored by operators to catch and mitigate any problems as quickly as possible. All root server organizations deploy redundant servers for the purpose of load balancing and high availability.

There are additional threats to the infrastructure that root servers rely on, such as physical hardware, power, cooling, physical security, and network connectivity that connects the systems to the Internet. Most instances of root servers are protected by significant organizational investments in physical infrastructure such as physical security, uninterruptable power supplies, computer room cooling, resilient network arrangements and backup equipment. Where these mitigations are not available, significant system redundancy is used to diversify these infrastructure requirements, such that failure of power/cooling/networking/etc. at one instance does not undermine the availability of that root server.

Route Hijacking

The Internet as a whole is critically dependent on the successful operation of the global routing table, currently negotiated via the Border Gateway Protocol (BGP). Significant resources have been expended within the IETF to develop secure routing technologies (RPKI and BGPsec specifically), but deployment is not yet ubiquitous. Some operators have utilized RPKI to strengthen their own infrastructure; however, there are potential risks with the centralized control of RPKI. As such, we believe the prudent course of action is for some operators to adopt RPKI and for other operators to wait until the protocol matures and the risks can be more fully understood and mitigated. Route hijacks are rare, but still represent a threat across many services on the Internet, including the root server address spaces. However, these are frequently monitored, rapidly detected and mitigations deployed to counteract potential hijacks. RSOs advertise the most specific route acceptable by global routing policy which makes route hijacking a bit more difficult. Due to heavy anycasting, BGP path length to a legitimate root server instance is usually quite low, which makes it more difficult to hijack routes to a route server instance for large sections of the Internet. The best defense to route hijacking is the use of DNSSEC validation which renders fake DNS data easily detectable and unusable.

Human Factors

Each RSO has their own Continuity of Operations Plan (COOP) with respect to personnel. This may include policies such as traveling on different flights/days or "on-call" hours. We recognize the importance of trust, value, and expertise within our staff and engineer these human factors in to our operations. The independence and diversity of COOPs among RSOs help ensure that the entire RSS is not vulnerable to any single attack against personnel.

Full, Immediate Compromise in the Availability of the Root Server System

If all instances of all Root Servers were to instantaneously become unavailable, the Internet would not immediately shut down. The use of caching by recursive resolvers would keep some root zone information available until the Time-To-Live (TTL) period of cached records expires. If the entire RSS became unavailable, the effect would first be seen by resolvers that did not have any required records from the root zone cached, and soon thereafter by resolvers that had required records in their cache that were about to expire. If the RSS was completely unavailable for an extended period, it is expected that the global set of recursive resolvers would begin to fail linearly over a period of the root zone record TTL (currently 48 hours). The number of Internet users affected by such an outage would *roughly* be proportional to the number of failed caching resolvers.