Postponing the Root KSK Roll

Matt Larson and Paul Hoffman
17 October 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
BACKGROUND	3
NEW INFORMATION IN SEPTEMBER 2017	3
FURTHER ANALYSIS BY OCTO RESEARCH	4
WHY DO VALIDATORS REPORT JUST KSK-2010?	5
ISSUES AND THOUGHTS	6
NEXT STEPS	6

Executive Summary

The root KSK rollover process began over two years ago when the ICANN organization collected opinions from DNS experts about how the roll should proceed. Those experts emphasized that, because of the large number of inherently unknown factors, a careful process should be followed before actually performing the rollover.

In September 2017, the ICANN organization and the technical community learned of four different factors that had the potential to negatively affect the number of resolvers that would be ready for the rollover. Based on these new revelations, which became apparent only weeks before the planned rollover date of 11 October 2017, the ICANN organization decided to postpone the rollover so the implications of the data and possible repercussions could be evaluated. This paper describes the new information and how continued work with the community will keep the KSK roll process moving forward.

Background

A full description of the KSK roll process, including how the process was created and the steps of the process, can be found at https://www.icann.org/kskroll. It is important to note that the process has always been open, as the ICANN organization reports to the community everything that is happening and is expected to happen in the future, and cautious, as all information from the community that affects the key roll process is evaluated with an eye to ensuring the security and stability of the Internet's DNS.

The transparency of the KSK roll process has given the technical community the ability to see what decisions we were making well before the decisions were put into motion. This approach was beneficial because the technical community reciprocated the openness. Its members gave us both their opinions as well as their data, which proved valuable in the formation of future decisions. Our cautious approach to each step in the process was based on the assumption that we had a good understanding of what to expect as we moved forward.

The full Operational Implementation Plan for the rollover[1] explains that the timing of every step is tentative; the process could be stopped at any time. Based on the recommendations from the KSK rollover Design Team[2], the steps can even be reversed if necessary; this option is described in the KSK Back Out Plan[3].

We are now in Phase D of that plan, including the "second packet size increase," which happened on 19 September 2017. This means that all the steps described in the operational plan before the rollover, have taken place. To date, no operational problems have been observed or reported to us.

New Information in September 2017

Four new pieces of information about the rollover appeared in September 2017:

[1] *See* https://www.icann.org/en/system/files/files/ksk-rollover-operational-implementation-plan-22jul16-en.pdf
[2] *See* https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf
[3] *See* https://www.icann.org/en/system/files/files/ksk-rollover-back-out-plan-22jul16-en.pdf

- Verisign, Inc. shared data that it had collected from the A and J root servers. This data comes from resolvers that are following the newly defined and implemented DNSSEC protocol extension defined in RFC 8145[4], which allows a resolver to indicate which trust anchors it is using. The data indicated that a surprising number of resolvers still had only the current root KSK, known as KSK-2010, as a trust anchor. This data afforded us the first objective measure of the number of resolvers that might start failing resolution after the rollover occurred.

- The Internet Systems Consortium (ISC), the developer of the BIND resolver, reported that some instances of BIND resolvers reporting trust anchor data were not in fact doing DNSSEC validation: an implementation issue in recent versions caused BIND to not follow the instructions in RFC 8145 correctly. As a result, an unknown number of resolvers reporting KSK-2010 were not actually performing validation.

- NLnet Labs, the developers of Unbound, revealed that some users of the Unbound resolver could correctly configure the software to follow the automatic trust anchor update protocol defined in RFC 5011[5], but still not have the new key, known as KSK-2017, on the day of the rollover. DNS resolution would fail for these users who start DNSSEC resolution for the first time within 30 days of the KSK rollover. NLnet Labs recently updated their software to handle this situation, but users of any earlier version of Unbound would still be affected.

- ISC also provided additional information about a problem that had been discovered earlier. Specifically, some BIND users who believe that their resolver has automatically updated its configuration to trust KSK-2017 were in fact only trusting KSK-2010. In some cases, BIND will start up and be unable to trust KSK-2017 but will provide no visible warning to that effect.

Further Analysis by OCTO Research

The Research group of ICANN's Office of the Chief Technology Officer (OCTO) began evaluating each of these four new issues as they appeared. After seeing Verisign's data, we analyzed similar query data from four additional root servers (B, D, F and L) and combined Verisign's data from A and J. This analysis was presented at the DNS Operations, Analysis, and Research Center (DNS-OARC) meeting in San Jose, California[6] on 29 September 2017 and that analysis is ongoing.

At the DNS-OARC meeting, we reported on traffic to these root servers from 1 September 2017 through 25 September 2017. The total number of unique addresses that reported trust anchor configuration data was 11,692, and the total number of unique addresses that exclusively reported KSK-2010 was 577. This data would suggest that about 5% of reporting resolvers would not ready for the KSK roll on 11 October 2017.

However, the analysis of these data is complicated. The 5% value does not include the variability introduced by the BIND issue that reports trust anchor data for resolvers that are not

[4] *See* https://tools.ietf.org/html/rfc8145
[5] *See* https://tools.ietf.org/html/rfc5011
[6] *See* https://indico.dns-oarc.net/event/27/

validating, so the number of validating resolvers might be lower (this BIND issue was reported after the Verisign data had been shared). On the other hand, many resolvers act as forwarders for queries from other resolvers, and forwarders make the situation look better if they obscure multiple validators behind the forwarder. Also, some resolvers have dynamic IP addresses, and this makes the situation look worse by inflating true number of sources.

Root KSK Roll Postponement

On 27 September 2017, the ICANN organization announced[7] the root KSK roll had been postponed until we can gather more information and understand the situation better. The length of the delay depends on the results of our investigation but will be at least three months. The design of the project dictates that when the rollover goes forward, it will do so on the 11th day of the first month of a quarter (either January, April, July, or October).

Further, prior to moving forward with the KSK roll, we will attempt to at least partially mitigate potential problems, using the new data that we have. We will reach out to the resolver operators whom we can identify as only using KSK-2010 and ask them if this is intentional on their part, suggesting they update their configurations and/or software to be ready for the rollover when it happens. We will also enlist the community's help in this outreach.

Why Do Validators Report Just KSK-2010?

Our analysis of some resolvers reporting trust anchor data, and analysis of the resolver software itself in our labs, confirms the following:

- Some resolvers running BIND report trust anchor data even if they are not validating. This means that a resolver might be reporting just KSK-2010 even if it is not trusting any key because validation is not enabled.

- Some resolvers were purposely configured to manually trust KSK-2010 and were never updated to use RFC 5011 automatic trust anchor updates, nor to manually also trust KSK-2017.

- There are implementation issues of the RFC 5011 protocol in some resolvers that prevent KSK-2017 from being trusted.

- Operator error can prevent KSK-2017 from being trusted. An actual example reported to us involved a Docker container with a resolver configured with KSK-2010 as a single trust anchor and automatic updates enabled. This resolver followed the automated update protocol and trusted KSK-2017 30 days after the container started, but reverted to trusting just KSK-2010 after the container was restarted.

[7] *See* https://www.icann.org/news/announcement-2017-09-27-en

Issues and Observations

We have always known that old configurations would be an issue at the time of the rollover, and have had a multi-year outreach program to try to convince operators with those old configurations to update to configurations that would support the KSK roll. However, until now, we never had any objective data reflecting the percentage might still be affected on the day of the rollover. Similarly, we worried that software issues and operator error were possible even though we didn't have hard evidence of this until September.

We are also very cognizant that the count of validators cannot be accurately mapped to the number of end users, and the impact on end users is what is most important. The root KSK roll Design Team understood this and based fallback criteria on the number of users affected, not number of resolvers. The Design Team's report referenced earlier, states:

Recommendation 16: Rollback of any step in the key roll process should be initiated if the measurement program indicated that a minimum of 0.5% of the estimated Internet end-user population has been negatively impacted by the change 72 hours after each change has been deployed into the root zone.

Determining the number of end users and systems that use a particular resolver is difficult, although we will be using data from a number of sources to help with this effort. We are also seeking query data from TLDs and other popular zones, which could help inform this part of the analysis.

Next Steps

The ICANN organization will attempt to contact the operators of systems reporting trust anchor information to the root servers that we believe are likely validating but are only using KSK-2010 as a trust anchor. We want to track down as many systems as possible to understand their behavior (is it an old configuration, a software implementation issue, operator error, something else) to help inform the decision for when to proceed with the rollover.

Depending on the outcome of our efforts to reach the operators of these systems, we will likely need to enlist the DNS technical community's help to identify and reach the systems reporting only KSK-2010 that we were unable to contact.

Similarly, because some resolvers act as forwarders, and those resolvers hide some possibly valuable data, we are asking resolver operators that forward to please start logging trust anchor reporting queries and then reach out to us.

We have already been working with software vendors to get the implementation issues described in this document addressed in future versions of their software.

As our analysis continues, we will keep the ICANN community up to date, explaining our findings and any plans we have for preparing to resume the rollover.