Rolling Forward: An Outlook on Future Root Rollovers

Position Paper for the IAB Workshop on *Design Expectations vs. Deployment Reality in Protocol Development*, 2019

Moritz Müller[1,2], *[3]

[1]SIDN Labs, [2]University of Twente,
[3] Other authors hidden due to double blind review

Abstract. The DNS Security Extensions (DNSSEC) add authenticity and integrity to *the* naming system of the Internet. To validate information in the DNS, resolvers need a copy of the cryptographic public key used to sign the root zone. This key was replaced for the first time in a process called *rollover* in October last year.
In order for the rollover to be successful, resolvers need to hold a copy of the new key. If not, resolvers might fail validation and render their clients effectively offline. We followed the process of the rollover starting in 2017 until the removal of the old key in 2019 using data, collected from multiple vantage points in the DNS ecosystem. Through this study we identified two key challenges during the rollover: (i) insufficient insight into validating resolvers and (ii) problems when distributing the DNSSEC trust anchor. In this paper we propose improvements to address both challenges in future rollovers. Especially the former might raise privacy and commercial concerns and require further thought from and debate in the community.

Workshop attendee confidential – study under double blind review

1 Introduction

The Domain Name System (DNS) is *the* naming system of the Internet. The DNS Security Extensions add a layer of authenticity and integrity to the DNS, using public key cryptography. Therefore, the root zone of the DNS is signed and resolvers need to hold a copy of the public key of the root zone to validate the signatures and configure it as a *trust anchor*. This public key, called Root Key Signing Key (KSK), was exchanged for the first time in 2018, an event referred to as a *rollover*.

A major challenge during a Root KSK rollover is the distribution of the new KSK to the validating resolvers. Resolvers that do not have the new key at the time of the rollover would fail validation and would not be able to serve any useful information to their clients. Responsible for distributing the new key is in most cases the protocol known as RFC 5011 [1]. It allows validators to automatically update their trust anchors through an in-band mechanism in the DNS.

To measure whether resolver successfully updated their trust anchors, two protocols have been standardized in the IETF: RFC 8145 [2] describes a protocol allowing DNSSEC validators to signal the keys in their trust anchor set *upstream*, for example to the root servers. RFC 8509, the so-called “Root Sentinel” [3], allows resolvers to signal *downstream* to their clients which trust anchors they use.

We are currently studying the signals from both protocols, before, during and after the rollover. Based on this analysis we have identified potential improvements to these protocols. Also, our analysis shows that not all resolvers have successfully picked up the new key. In the remainder of this paper we discuss which features an *ideal* telemetry protocol should have. Some of the features raise privacy and commercial concerns and require discussion. We further describe how the Root KSK could be reliably distributed in the future to also serves rather new trends, like the proliferation of container technologies and validation at end-clients.

2 Improving Telemetry

We study RFC 8145 signals during the 2018 Root KSK rollover with the help of two data sets: (i) all trust anchor signals received by A/J Root since January 10th, 2017, and (ii) trust anchor signals provided to ICANN by most of the root server operators. For analyzing RFC 8509 signals we actively query resolvers using the Luminati Proxy network [4]. In total we analyzed the signals of more than 1 million sources during different stages of the rollover.

During our measurements, we identified some draw backs at both protocols. The signal of RFC 8145 turned out to be difficult to interpret for several reason: first, in case of the root rollover, only the root servers can collect the telemetry and it is not possible to query a failing resolver to debug the issue. Also, if a failing resolver is identified we cannot estimate whether this failure is actually relevant for users. Last, the signal of RFC 8145 received at the root servers might not have its origin at the sending resolver but might have only been forwarded. The actual failing resolvers is therefore hidden. Nevertheless, *without RFC 8145* ICANN and the DNS community would have been without *any* signal and some problems would have stayed in the dark.

In comparison to RFC 8145, the Root Sentinel (RFC 8509) can be triggered by active measurements from the client of the resolver. Thus, users can check themselves whether their resolver has the latest keys configured. For our study we ran active measurements, and despite its then limited deployment, they provided useful signals. Nevertheless, while RFC 8509 addresses the first limitation of RFC 8145, it is still sharing the others. For example, a client cannot detect whether its Root Sentinel query sent to resolvers at a large ISP is actually handled by a local forwarder.

So while both protocols can provide some helpful signal during rollovers we recommend incremental improvements to RFC 8145 and RFC 8509. First, an ideal telemetry protocol should include the IP address that handled or the signal query, which would enable the detection of DNS forwarding. Second, resolvers could give some indication about the number of clients it serves, which could make it easier to estimate the impact of failures of resolvers. For example, this could have given the community the confidence that most *important* resolvers were indeed ready for last year's rollover. We note, however, that especially the latter recommendation raises privacy and commercial concerns and we recommend further discussing them with the community.

3 Trust Anchor Distribution

While analyzing the signals from RFC 8145 and RFC 8509 and with the help of other active and passive measurements during the last Root KSK rollover we found that *some* resolvers did not configure the correct key. Responsible for distributing the new key is in most cases the protocol RFC 5011. It allows validators to automatically update their trust anchors through an in-band mechanism in the DNS. Validators that do not update their trust anchor will fail validation after a rollover and while our study suggests that RFC 5011 worked generally as intended, we noticed that not all resolvers correctly picked up the new key.

From public discussions and by reaching out to affected operators, we found that in some cases RFC 5011 failed due to lacking file-system permissions or due to teardown and reinitialisation of systems like containers or virtual machines. We expect that the latter issue might become even bigger, considering the rising adoption of container technologies, which was not envisioned when RFC 5011 got standardized more than 11 years ago. Another trend, which we also encountered during our studies, is DNSSEC validation in end user applications. We observed that keys necessary for validation are often hard-coded directly in the source code without providing mechanisms to update those keys in case of a rollover. These trends raise the question if RFC 5011 is still the best way to update trust-anchors in the future.

We therefore advocate for an alternative for trust-anchor distribution, relying on the underlying operating system to provide the recent keys. Some operating systems like Debian Linux started doing this already and we believe that this is a scalable solution for providing keys to end-user applications. At the same time, we strongly urge against trust-anchors hard-coded in the code of the software.

References

1. M. StJohns, "Automated Updates of DNS Security (DNSSEC) Trust Anchors," RFC 5011 (Internet Standard), RFC Editor, Fremont, CA, USA, pp. 1–14, Sep. 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5011.txt
2. D. Wessels, W. Kumari, and P. Hoffman, "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)," RFC 8145 (Proposed Standard), RFC

Editor, Fremont, CA, USA, pp. 1–13, Apr. 2017, updated by RFC 8553. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8145.txt

3. G. Huston, J. Damas, and W. Kumari, "A Root Key Trust Anchor Sentinel for DNSSEC," RFC 8509 (Proposed Standard), RFC Editor, Fremont, CA, USA, pp. 1–19, Dec. 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8509.txt
4. Luminati IO, "Residential IP and Proxy Service for Businesses," https://luminati.io/, May 2018.