Root KSK Roll Delay Update

DNSSEC-For-Beginners

Roy Arends, Principal Research Scientist

29 October 2017

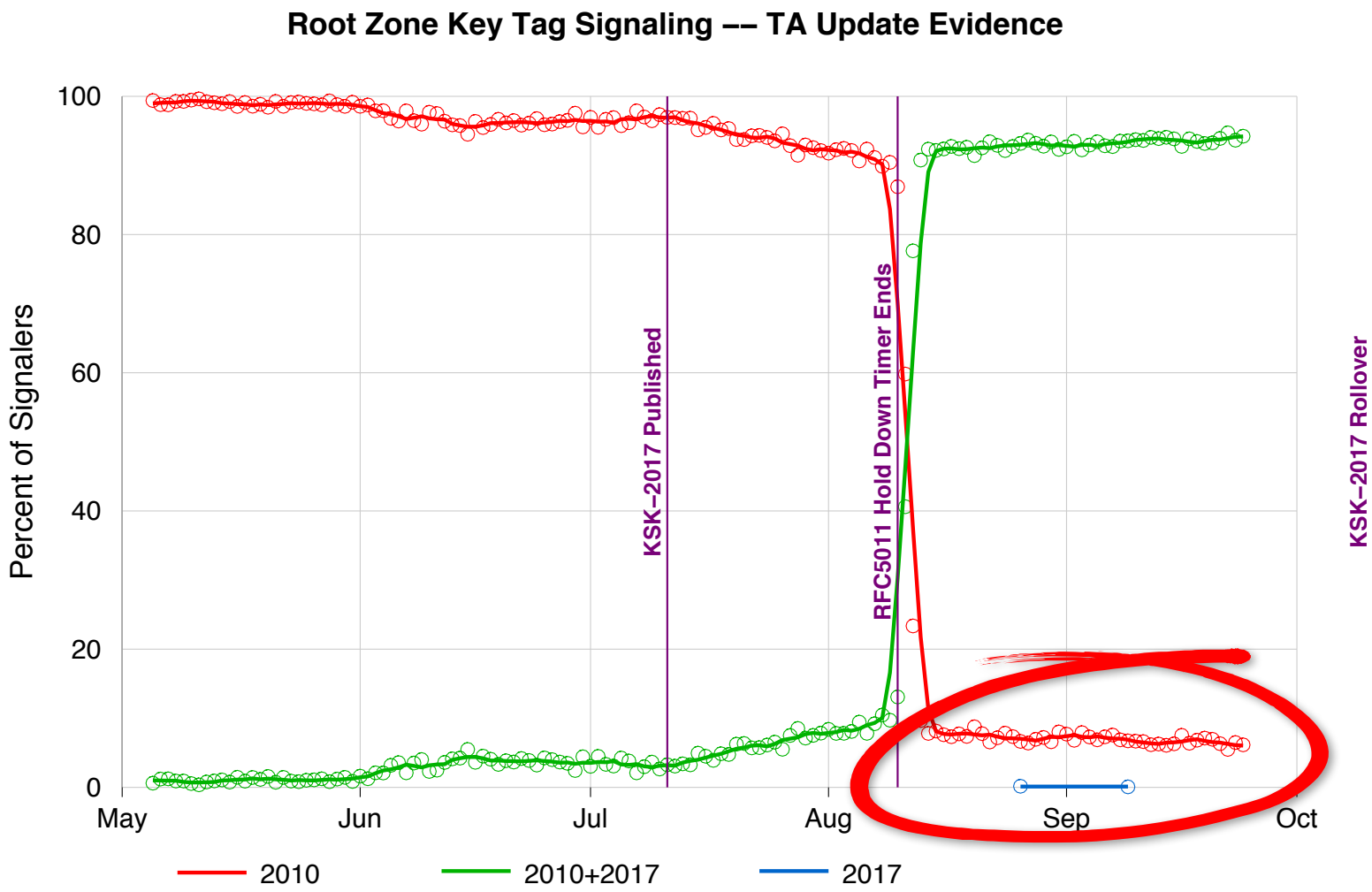
Background

- When you validate DNSSEC signed DNS records, you need a Trust Anchor.
  - A Trust Anchor is a Public Key.
- Public Keys should not live forever.
- These Trust Anchors probably should be periodically renewed (rolled).
  - You can do this automatically or manually.
- However, there was no way for us (ICANN) to check if you have the right key configured.
- Therefore, a multi-year design and outreach effort ensued:
  - Design-team, blogs, outreach, presentations in various venues, plans, vendors and governments were contacted, etc., etc.

The Process

- **11 July 2017**: Introduce the new KSK-2017.
  - Monitor if there are fundamental changes in root-server traffic
  - If not, continue, else fall back.
- **10 August 2017**: “30 day hold-down period ends”
  - Monitor if there are fundamental changes in root-server traffic.
  - If not, continue, else fall back.
- **19 September 2017**: DNSKEY Response size increased due to standard ZSK roll
  - Monitor if there are fundamental changes in root-server traffic.
  - If not, continue, else fall back.

Hey! There's data! Wait. What?



Further analysis by OCTO Research

- ICANN OCTO Research did an analysis similar to Duane's
  - **6.02% of reporting validators were not ready for the KSK roll on 11 October 2017**
  - Dynamic resolver IPs make the situation look worse by inflating true number of sources
  - Resolvers behind forwarders make the situation look better as they obscure multiple validators behind the forwarder

- Multiple reasons suspected or confirmed:
  1. BIND reports trust anchors even if not validating
  2. BIND's *trusted-keys* is used instead of *managed-keys* or *dnssec-validation auto*
  3. Some resolvers are in front of validating forwarders.
  4. Operator error, like Docker container keeps booting up with only KSK-2010 and starts 5011 all over again

- We worried bugs and operator error were possible but didn't have evidence until now

Back to the plan and process

- 19 September 2017: DNSKEY Response size increased due to standard ZSK roll
  - Monitor if there are fundamental changes in root-server traffic.
  - If not, continue, else fall back.
- We had received Verisign's report and corroborated it with our own data.
- From the Operational Plan:

  "*The Root Zone Management Partners might also decide to extend any phase for additional quarters. For example, if new information indicates that the next phase may lead to complications, the current phase would be prolonged. This is referred to as an extend scenario.*"
- 27 September 2017: "Extend" scenario kicks in
  - ICANN Announces that the root KSK Rollover is delayed

Issues

- We do not know how representative the set of validators reporting key tag data is compared to the set of all validators
- Validators != end users (or “end systems”), and the impact on end users is what is most important
  - The design team recognized this
- Determining number of end users/systems for a given resolver is hard
  - APNIC’s Google Ad experiment platform-based data will help
- Mitigation is hard
  - We’ve already had a multi-year campaign to reach operators
  - Implementation-specific problems don’t make the problem easier

Next Steps

- We postponed the root KSK roll until we can gather more information and understand the situation better
  - The delay will be at least one quarter
  - We have not yet determined how many quarters to delay
- We will at least partially mitigate
  - Contractor hired to try to track down the first 500 resolvers based on IP addresses and understand why misconfiguration is occurring
  - Data collection continues
- We'll need to re-engage/re-tune the communications plan
  - Maybe "PLEASE DO **NOT** REMOVE KSK-2017!!"?

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann