Roll, Roll, Roll Your Root

A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover

ACM Internet Measurement Conference 2019 – Amsterdam, 2019-10-21

Moritz Müller\textsuperscript{3,4}, Matthew Thomas\textsuperscript{6}, Duane Wessels\textsuperscript{6}, Wes Hardaker\textsuperscript{5}, Taejoong Chung\textsuperscript{2}, Willem Toorop\textsuperscript{1}, Roland van Rijswijk-Deij\textsuperscript{1,4}

\textsuperscript{1}NLnet Labs, \textsuperscript{2}Rochester Institute of Technology, \textsuperscript{3}SIDN, \textsuperscript{4}University of Twente, \textsuperscript{5}USC/Information Sciences Institute, \textsuperscript{6}Verisign
Introduction

• The DNS root is signed using DNSSEC
• Validators need the public key of the Root and configure it as trust anchor
• In 2018, the trust-anchor was replaced (or “rolled”) for the first time

• The old public key: KSK-2010
• The new public key: KSK-2017
Why is rolling hard?

• No key $\rightarrow$ No validation $\rightarrow$ No DNS responses
• Every validator needs to have KSK-2017, but:
  • Validators use hard-coded keys
  • Containers challenge key update
  • People tend to forget about DNS
Resolver Telemetry: RFC 8145

- The goal: estimating how many validators had KSK-2017
- The solution: resolvers signal to the root which keys they trust
- Data from ICANN from A, B, and J root
- Signals from up to 100,000 validators daily
ICANN resumes rollover process
18 Sep 2018

ICANN halts rollover process
27 Sep 2017

KSK-2017 published in Root Zone
11 Jul 2017

The Rollover
11 Oct 2018

Revocation of KSK-2010
11 Jan 2019

KSK-2010 removed from Root Zone
22 Mar 2019

TIMELINE

I

II

STOP

III

IV

V

VI
Before the Rollover

I

KSK-2017 published in Root Zone
11 Jul 2017

II

STOP

III

ICANN halts rollover process
27 Sep 2017

IV

ICANN resumes rollover process
18 Sep 2018

V

VI
Uptake of KSK-2017

The graph shows the uptake of KSK-2017 over the months May to October. The fraction of signallers using KSK-2017 is compared to KSK-2010. KSK-2017 was added to the zone in August 2017, as indicated by the shaded area.

Key:
- **KSK-2010**: Red line
- **KSK-2017**: Blue line

**Notes:**
- **RFC 5011 add hold-down**: Indicates the time period in August 2017 when RFC 5011 was added, causing a significant increase in the usage of KSK-2017.
Uptake of KSK-2017

8% of resolvers don’t have KSK-2017

Fraction of signallers

KSK-2010
KSK-2017

RFC 5011 added hold-down

KSK-2017 added to zone

2017

May Jun Jul Aug Sep Oct
Zooming in on resolvers that only have KSK-2010

• Lots of RFC 8145 sources sent only one signal
• Many sent only a few queries

<table>
<thead>
<tr>
<th>Query</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>_ta-4a5c</td>
<td>15,447</td>
</tr>
<tr>
<td>.</td>
<td>9,182</td>
</tr>
<tr>
<td>VPN domain</td>
<td>3,156</td>
</tr>
<tr>
<td>VPN alternate domain</td>
<td>415</td>
</tr>
<tr>
<td>_sip._udp.otherdomain</td>
<td>86</td>
</tr>
</tbody>
</table>
Zooming in on resolvers that only have KSK-2010
Zooming in on resolvers that only have KSK-2010

Fraction of RFC 8145 signallers

IPv4
IPv6

Feb '18  Apr '18  Jun '18  Aug '18  Oct '18  Dec '18

Actual rollover
Takeaways from before the Rollover

• **Most** validators correctly picked up KSK-2017
• But **one single application** can influence the trust-anchor signal
• Validation in applications might become more common
  → **Influence on telemetry**
During the Rollover

The Rollover
11 Oct 2018
The User’s Perspective: RIPE Atlas

• The goal: measuring how users perceive the rollover
• The approach: Measuring with all RIPE Atlas probes once per hour
  a) If they have cached KSK-2017
  b) If they validate correctly

• We observed 35,719 resolver addresses in 3,141 ASes and correlated failing resolvers with DNSKEY queries with DITL data
Activating KSK-2017

% VPs with Key Cached

Oct 11−16:00h
Oct 12−00:00h
Oct 12−08:00h
Oct 12−16:00h
Oct 13−00:00h
Oct 13−08:00h
Oct 13−16:00h
Oct 14−00:00h
Oct 14−08:00h
Oct 14−16:00h

2017

KSK−2010
KSK−2017
Activating KSK-2017

Large resolvers start validating with KSK-2017

% VPs with Key Cached

Oct 11–16:00h
Oct 12–00:00h
Oct 12–08:00h
Oct 12–16:00h
Oct 13–00:00h
Oct 13–08:00h
Oct 13–16:00h
Oct 14–00:00h
Oct 14–08:00h
Oct 14–16:00h

KSK–2010
KSK–2017

2017
Failure Modes

Failing and then Insecure

0 20 40 60
1000 2000 3000
0 500 1000

Oct 11 − 00:00 Oct 11 − 08:00 Oct 11 − 16:00 Oct 12 − 00:00 Oct 12 − 08:00 Oct 12 − 16:00 Oct 13 − 00:00 Oct 13 − 08:00 Oct 13 − 16:00 Oct 14 − 00:00 Oct 14 − 08:00 Oct 14 − 16:00

I STOP IV V VI
Validation Failure Modes

- Failing and then Insecure
- Failing and then Recover

Oct 11 – 00:00 to Oct 14 – 16:00
Validation Failure Modes

- Failing and then Insecure
- Failing and then Recover
- Failing and then Bogus
Reaction to Validation Failures

35,719 unique resolver sources in RIPE Atlas

970 secure before, bogus after rollover

747 secure before, insecure after rollover
Reaction to Validation Failures

35,719 unique resolver sources in RIPE Atlas

- 970 secure before, bogus after rollover
- 747 secure before, insecure after rollover
- 519 sending excess DNSKEY queries
- 359 sending 1.5x more DNSKEY queries after rollover
Reaction to Validation Failures

35,719 unique resolver sources in RIPE Atlas

970 secure before, bogus after rollover
747 secure before, insecure after rollover

519 sending excess DNSKEY queries

359 sending 1.5x more DNSKEY queries after rollover

218 fixed within 1h
138 fixed after 1h
3 never fixed

I  STOP  IV  V  VI
Broadband restored to Eir customers after outage
Company says problem with DNS server led to outage across the country


EIR Outage - Was it DNS(SEC)?

Queries per day

Rollover

Revocation

Removal

Aug '18  Sep '18  Oct '18  Nov '18  Dec '18  Jan '19  Feb '19  Mar '19  Apr '19
EIR Outage - Was it DNS(SEC)?

Massive increase after the rollover

Queries per day

0 - 25000 - 50000 - 75000 - 100000 - 125000

Aug '18 - Sep '18 - Oct '18 - Nov '18 - Dec '18 - Jan '19 - Feb '19 - Mar '19 - Apr '19
EIR Outage - Was it DNS(SEC)?

Mysterious bump after removal of KSK-2010
Takeaways from *during* the Rollover

- **Few** resolvers had **serious problems**
- The ones that had problems **recovered fast**
- Less than **0.01%** of the resolvers we monitored experienced problems
After the Rollover

Revocation of KSK-2010
11 Jan 2019

KSK-2010 removed from Root Zone
22 Mar 2019
Increase in DNSKEY queries

- **STOP**: Sep '18
- **Rollover**: Nov '18
- **Revocation**: Feb '19
- **Removal**: Apr '19

Queries per day

- **Aug '18**: 0 M
- **Sep '18**: 0 M
- **Oct '18**: 0 M
- **Nov '18**: 0 M
- **Dec '18**: 0 M
- **Jan '19**: 0 M
- **Feb '19**: 0 M
- **Mar '19**: 0 M
- **Apr '19**: 1250 M
Increase in DNSKEY queries

- **Aug '18**: Initial baseline
- **Sep '18**: Minor increase
- **Oct '18**: Steady baseline
- **Nov '18**: Partially expected increase
- **Dec '18**: Slight increase
- **Jan '19**: Continued steady baseline
- **Feb '19**: Revocation event
- **Mar '19**: Steady increase
- **Apr '19**: Significant increase

Events:
- **Rollover (1)**: Partially expected increase
- **Revocation (2)**: Decrease
- **Removal (3)**: Spike in queries
- **Removal (4)**: Decrease
Increase in DNSKEY queries

Queries per day

- **Aug '18**: Baseline
- **Sep '18**: Slight increase
- **Oct '18**: Steady increase
- **Nov '18**: Significant increase (Partially expected increase)
- **Dec '18**: Plateau
- **Jan '19**: Continuous rise
- **Feb '19**: Very unexpected increase
- **Mar '19**: Continued rise
- **Apr '19**: Peak (Removal)

- **Rollover**
- **Revocation**

I STOP IV V VI
Increase in DNSKEY queries

Queries per day

- **Aug '18**: Rollover
- **Nov '18**: Partially expected increase
- **Jan '19**: Revocation
- **Mar '19**: 7% of total query load
- **Apr '19**: Removal

Very unexpected increase

Stop
Increase in DNSKEY queries after revocation

- ZSK rollover
- RFC 5011 hold-down for revocation
- KSK-2010 revoked

Fraction of traffic

<table>
<thead>
<tr>
<th>Fraction of traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.100</td>
</tr>
<tr>
<td>0.075</td>
</tr>
<tr>
<td>0.050</td>
</tr>
<tr>
<td>0.025</td>
</tr>
<tr>
<td>0.000</td>
</tr>
</tbody>
</table>

Jan '19      Feb '19      Mar '19

Graph showing the increase in DNSKEY queries after revocation, with specific timestamps and fractions of traffic.
Increase in DNSKEY queries after revocation

ZSK rollover

RFC 5011 hold-down for revocation

KSK-2010 revoked

Most root servers see the increase
Increase in DNSKEY queries after revocation

Most root servers see the increase

But not all of them
Who’s behind the query floods?

• DNS CHAOS queries to sources reveal mostly older versions of BIND

• Outreach
  • A large French cloud hosting provider confirmed a source running BIND 9.8.2 on CentOS
  • Large midwestern university confirmed DNS lab exercise and provided BIND config
Reproducing Key Floods with BIND

- Conditions for reproducing DNSKEY floods with BIND:
  - DNSSEC managed keys contains KSK-2010, but not KSK-2017
  - The `dnssec-enable` flag was set to false
  - The `dnssec-validation` flag was unset, leaving it in its default state of “yes.”
Reproducing Key Floods with BIND

• Conditions for reproducing DNSKEY floods with BIND:
  • DNSSEC managed keys contains KSK-2010, but not KSK-2017
  • The dnssec-enable flag was set to false
  • The dnssec-validation flag was unset, leaving it in its default state of “yes.”

Bursts occur only occasionally
Resolver Telemetry: RFC 8509 “Root Sentinel”

The return of KSK-2010
Resolver Telemetry: The return of KSK-2010

![Diagram showing the fraction of signallers over time with Rollover, Revocation, and Removal phases highlighted.](image-url)
Takeaways from *after* the Rollover

- **No one** expected the massive flood of DNSKEY queries
- Trust anchor management comes in **different shapes and colors**
- Shipping trust anchors with software has **long-lasting effects**
Discussion
Do we need to improve telemetry?

- RFC 8145 and RFC 8509 are useful but should be improved
  - Allowing to identify the true source of a signal
  - Provide an estimate for how many users a signal represents
Do we need to improve telemetry?

• RFC 8145 and RFC 8509 are useful but should be improved
  • Allowing to identify the true source of a signal
  • Provide an estimate for how many users a signal represents

Do we need to change trust anchor management?

E.g. shipping TAs centrally in OSes?
Conclusions and broader Lessons

• The rollover was a **success**
• **Independent analysis** and measurements on the internet are valuable
• Telemetry must be kept in mind **at an early stage** of protocol development
• Trust anchors should be **managed centrally**
Conclusions and broader Lessons

• The rollover was a **success**
• **Independent analysis** and measurements on the internet are valuable
• Telemetry must be kept in mind **at an early stage** of protocol development
• Trust anchors should be **managed centrally**

---

**Questions, suggestions, comments?**

Data available at

*https://github.com/SIDN/RollRollRollYourRoot*

Contact

Moritz Müller | moritz.muller@sidn.nl | sidnlabs.nl