Roll, Roll, Roll Your Root
A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover
RoN++ Meeting 2019 – Utrecht, 2020-01-08

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 Labs, \textsuperscript{4}University of Twente, \textsuperscript{5}USC/Information Sciences Institute, \textsuperscript{6}Verisign
Introduction

• DNSSEC brings **integrity** to the DNS
• 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 key: **KSK-2010**
• The new key: **KSK-2017**
Introduction

• DNSSEC brings **integrity** to the DNS
• 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 key: **KSK-2010**
• The new key: **KSK-2017**

Recursive Resolver

a.gtld-servers.net.
b.gtld-servers.net.
...

Root
Introduction

• DNSSEC brings integrity to the DNS
• 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 key: KSK-2010
• The new key: KSK-2017
Introduction

• DNSSEC brings **integrity** to the DNS
• 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 key: **KSK-2010**
• The new key: **KSK-2017**
Introduction

• DNSSEC brings **integrity** to the DNS
• 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 key: **KSK-2010**
• The new 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
Timeline

I
KSK-2017 published in Root Zone
11 Jul 2017

II
ICANN halts rollover process
27 Sep 2017

STOP

III
The Rollover
11 Oct 2018

IV
ICANN resumes rollover process
18 Sep 2018

V
Revocation of KSK-2010
11 Jan 2019

VI
KSK-2010 removed from Root Zone
22 Mar 2019
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.  

---

ICANN resumes rollover process
18 Sep 2018

ICANN halts rollover process
27 Sep 2017

KSK-2017 published in Root Zone
11 Jul 2017
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
Uptake of KSK-2017

Fraction of signallers

May Jun Jul Aug Sep Oct

KSK-2010
KSK-2017

0.00 0.25 0.50 0.75 1.00

RFC 5011
add
hold-down

KSK-2017 added to zone

STOP
Uptake of KSK-2017

8% of resolvers don’t have KSK-2017

Fraction of signallers

KSK-2010
KSK-2017

RFC 5011 added to zone
KSK-2017 added to zone
hold-down

May Jun Jul Aug Sep Oct

IV
V
VI

STOP
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>

Domains, queried by resolvers
Zooming in on resolvers that only have KSK-2010

Fraction of RFC 8145 signallers

IPv4
IPv6

Actual rollover

Feb '18 Apr '18 Jun '18 Aug '18 Oct '18 Dec '18
Zooming in on resolvers that only have KSK-2010
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

KSK−2010
KSK−2017

Stop
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

2017

KSK–2010
KSK–2017

I
STOP
IV
V
VI
Reaction to Validation Failures

35,719 unique resolver sources in RIPE Atlas

34,002 always secure or always insecure
Reaction to Validation Failures

35,719 unique resolver sources in RIPE Atlas

- **34,002** always secure or always insecure
- **970** secure before, bogus after rollover
- **747** secure before, insecure after rollover
Reaction to Validation Failures

- **35,719** unique resolver sources in RIPE Atlas
- **34,002** always secure or always insecure
- **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

- 34,002 always secure or always insecure
- 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
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)?

Massive increase after the rollover

Queries per day

Aug '18 | Sep '18 | Oct '18 | Nov '18 | Dec '18 | Jan '19 | Feb '19 | Mar '19 | Apr '19

STOP
EIR Outage - Was it DNS(SEC)?

Mysterious bump after removal of KSK-2010
After the Rollover

Revocation of KSK-2010
11 Jan 2019

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

Queries per day

Aug '18  Sep '18  Oct '18  Nov '18  Dec '18  Jan '19  Feb '19  Mar '19  Apr '19

0 M  250 M  500 M  750 M  1 000 M  1 250 M

Rollover  Revocation  Removal

1  2  3  4
Increase in DNSKEY queries

- **Partially expected increase**
- **Revocation**
- **Removal**

Queries per day:
- Aug '18
- Sep '18
- Oct '18
- Nov '18
- Dec '18
- Jan '19
- Feb '19
- Mar '19
- Apr '19
Increase in DNSKEY queries

Queries per day

Aug '18  Sep '18  Oct '18  Nov '18  Dec '18  Jan '19  Feb '19  Mar '19  Apr '19

1 250 M
750 M
0 M

STOP

Rollover

Very unexpected increase

Revocation

Partially expected increase

Removal

Very unexpected increase

Removal

Removal
Increase in DNSKEY queries

- **Rollover** (Nov '18): Partially expected increase
- **Revocation** (Feb '19): Very unexpected increase
- **Removal** (Mar '19): 7% of total query load

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: 1,250 M

Note: The graph shows a significant increase in DNSKEY queries starting from Feb '19, reaching 7% of the total query load.
Increase in DNSKEY queries

- 1 M increase in DNSKEY queries:
  - Partially expected increase
  - 7% of total query load

- 1.25 G increase in DNSKEY queries:
  - Very unexpected increase

Return to load after rollover
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: The return of KSK-2010
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
Bonus Slides
Increase in DNSKEY queries after revocation

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

Most root servers see the increase

But not all of them

ZSK rollover

RFC 5011 hold-down for revocation

KSK-2010 revoked

Fraction of traffic

Jan '19  Feb '19  Mar '19
Resolver Telemetry: RFC 8509 “Root Sentinel”

![Graph showing resolver telemetry data with labels for Rollover, Revocation, and Removal. The graph plots the number of resolvers over time from August 2018 to August 2019. Two lines represent KSK-2010 and KSK-2017.]
Resolver Telemetry: RFC 8509 “Root Sentinel”

The return of KSK-2010
Failure Modes

Failing and then Insecure

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
Validation Failure Modes

- Failing and then Insecure
- Failing and then Recover
- Failing and then Bogus