Roll, Roll, Roll Your Root

A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover

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

Moritz Müller³,⁴, Matthew Thomas⁶, Duane Wessels⁶, Wes Hardaker⁵, Taejoong Chung², Willem Toorop¹, Roland van Rijswijk-Deij¹,⁴

¹NLnet Labs, ²Rochester Institute of Technology, ³SIDN Labs, ⁴University of Twente, ⁵USC/Information Sciences Institute, ⁶Verisign
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**
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

STOP

ICANN halts rollover process
27 Sep 2017

II

The Rollover
11 Oct 2018

ICANN resumes rollover process
18 Sep 2018

III

Revocation of KSK-2010
11 Jan 2019

IV

KSK-2010 removed from Root Zone
22 Mar 2019

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. 
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

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

0.00 0.25 0.50 0.75 1.00
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
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
Zooming in on resolvers that only have KSK-2010
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 14–00:00h
Oct 14–08:00h
Oct 14–16:00h

KSK-2010
KSK-2017
Activating KSK-2017

Large resolvers start validating with KSK-2017
Reaction to Validation Failures

- 35,719 unique resolver sources in RIPE Atlas
- 34,002 always secure or always insecure
- 970 always secure, insecure after rollover
- 519 sending 1.5x more DNSKEY queries after rollover
- 359 secure before, bogus 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

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

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


File photograph: Maxwells

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

0 | 25000 | 50000 | 75000 | 100000 | 125000

STOP

I | IV | V | VI
EIR Outage - Was it DNS(SEC)?

Queries per day

- Rollover
- Revocation
- Removal

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
Increase in DNSKEY queries

- **Aug '18**: Rollover
- **Nov '18**: Partially expected increase
- **Dec '18**: Increase
- **Jan '19**: Revocation
- **Feb '19**: Increase
- **Mar '19**: Revocation
- **Apr '19**: Removal
Increase in DNSKEY queries

- **Partially expected increase**
- **Very unexpected increase**

Queries per day:
- 0 M
- 250 M
- 500 M
- 750 M
- 1 000 M
- 1 250 M

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

Events:
- Rollover
- Revocation
- Removal

Stop

Page 33
Increase in DNSKEY queries

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

Queries per day

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

**Graph:**
- **Rollover**
- **Revocation**
- **Removal**

**Timeline:**
- **I**: STOP
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.”
Resolver Telemetry: The return of KSK-2010

Fraction of signallers


Rollover Revocation Removal

KSK–2010 KSK–2017
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
Bonus Slides
Increase in DNSKEY queries after revocation

Most root servers see the increase

Fraction of traffic

Jan '19  Feb '19  Mar '19

ZSK rollover

RFC 5011 hold–down for revocation

KSK–2010 revoked

0.100
0.075
0.050
0.025
0.000

0.000 0.025 0.050 0.075 0.100
Increase in DNSKEY queries after revocation

Most root servers see the increase

But not all of them

Fraction of traffic

Jan '19 Feb '19 Mar '19

0.100-

0.075-

0.050-

0.025-

0.000-

ZSK rollover

RFC 5011 hold–down for revocation

KSK–2010 revoked

0.000

0.025

0.050

0.075

0.100

0.025

0.050

0.075

0.100
Resolver Telemetry: RFC 8509 “Root Sentinel”
Resolver Telemetry: RFC 8509 “Root Sentinel”

The return of KSK-2010
Failure Modes

Failing and then Insecure
Validation Failure Modes

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

Failing and then Recover

Failing and then Insecure

52
Validation Failure Modes

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