The KSK roll: From Concern to Calm(ish)

Wes Hardaker

2017-08-30
Overview

- My Paranoia
- Face Your Fears
- Reality
My Initial Paranoia

► What happens if a fraction of the world falls off the net?
► What happens if their resolvers go crazy?
► What happens if they send millions of requests?
My Initial Paranoia

- What happens if a fraction of the world falls off the net?
- What happens if their resolvers go crazy?
- What happens if they send millions of requests?
- It happened before, after all...

(Graph created by George Michaelson)
Face your fears

- Paranoia led to analyzing many days of data
  - Previous: misconfigured VPN software
  - Today: my failure to find much else
Who’s in Danger?

To find out who’s in trouble, we need to know:

1. What keys a validator is using
   - RFC8145
   - KSK signaling
   - Neither are complete signals!

2. Are they validating
   - Is this possible?
Background: *(Expected)* Resolver Behavior

- Resolver \( \text{www.example.com/A} \) ⇒ the root
Background: *(Expected)* Resolver Behavior

- Resolver \( \frac{\text{www.example.com/A}}{} \Rightarrow \text{the root} \)

- Resolver \( \frac{\text{com/NS, com/DS, glue}}{} \Leftarrow \text{the root} \)
Background: *(Expected)* Resolver Behavior

- Resolver \( \text{www.example.com}/A \) the root
- Resolver \( \text{com/NS, com/DS, glue} \) the root
- Frequent: Resolver \( \text{com/DS} \) the root
  - Unclear which resolvers do (bind, eg, does)
Background: (Expected) Resolver Behavior

- Resolver $\frac{www.example.com/A}{\Rightarrow}$ the root

- Resolver $\frac{com/NS, com/DS, glue}{\Leftarrow}$ the root

- Frequently: Resolver $\frac{com/DS}{\Rightarrow}$ the root
  - Unclear which resolvers do (bind, eg, does)

- Validating resolver hypothesis:
  - $\sim50\%$ of queries should be for TLD/DS
Data Cleaning

- First step: ignore non-root-zone queries
- Example: Chrome sends random strings (orange line)

Graph created by USC student Haoyu Jia
Results: Percentage of DS Queries

Hosts sending at least 5 DS
Next question...

- Our hypothesis appears correct sometimes
Next question...

- Our hypothesis appears correct sometimes
- Let’s narrow further to:
  - Sources sending $DS > 25\%$ and $%DS < 80\%$
  - On September 25, 2018
Next question...

- Our hypothesis appears correct sometimes
- Let’s narrow further to:
  - Sources sending \( DS > 25\% \) and \( DS < 80\% \)
  - On September 25, 2018
- Next question:
  - Which of these were \( KSK2010\text{-only} \) validators
Next question...

- Our hypothesis appears correct sometimes
- Let’s narrow further to:
  - Sources sending $DS > %25$ and $%DS < %80$
  - On September 25, 2018

- Next question:
  - Which of these were *KSK2010-only* validators

- Matching resolvers: 45,806
Next question...

- Our hypothesis appears correct sometimes
- Let’s narrow further to:
  - Sources sending \( DS > \%25 \) and \( %DS < \%80 \)
  - On September 25, 2018
- Next question:
  - Which of these were \textit{KSK2010-only} validators
- Matching resolvers: 45,806
- Total signaling support for KSK2016 (via RFC8145): 420
Next question...

- Our hypothesis appears correct sometimes

- Let’s narrow further to:
  - Sources sending $DS > \%25$ and $%DS < %80$
  - On September 25, 2018

- Next question:
  - Which of these were *KSK2010-only* validators

- Matching resolvers: 45,806

- Total signaling support for KSK2016 (via RFC8145): 420

- Total signaling only KSK2010 (via RFC8145):
Next question...

- Our hypothesis appears correct sometimes
- Let’s narrow further to:
  - Sources sending DS > %25 and DS < %80
  - On September 25, 2018
- Next question:
  - Which of these were KSK2010-only validators
- Matching resolvers: 45,806
- Total signaling support for KSK2016 (via RFC8145): 420
- Total signaling only KSK2010 (via RFC8145): 12
Our hypothesis appears correct sometimes

Let’s narrow further to:
  - Sources sending DS > %25 and %DS < %80
  - On September 25, 2018

Next question:
  - Which of these were KSK2010-only validators

Matching resolvers: 45,806

Total signaling support for KSK2016 (via RFC8145): 420

Total signaling only KSK2010 (via RFC8145): 12

Down from 18 the month before!
Next question...

- What DS requests were they sending?
- A reasonable resolver would...
  - Send a DS request only for the TLD name
  - e.g. com/DS and never example.com/DS
Next question... 

- What DS requests were they sending?
- A reasonable resolver would...
  - Send a DS request only for the TLD name
  - e.g. com/DS and never example.com/DS
- Are resolvers really reasonable?
Next question...

- What DS requests were they sending?
- A reasonable resolver would...
  - Send a DS request only for the TLD name
  - e.g. com/DS and never example.com/DS

- Are resolvers really reasonable?

- Hint: No.
What actually happened?

What did real life look like?
Just before the roll
Just starting the roll
Much later

PHEW
Conclusions

- The world is finally getting better at
  - updating software
  - updating config
- I believe the extra year was very wise
- Resolvers behave strangely
  - Looking forward to the RSSAC caucus resolver study!
Conclusions

- The world is finally getting better at
  - updating software
  - updating config
- I believe the extra year was very wise
- Resolvers behave strangely
  - Looking forward to the RSSAC caucus resolver study!
- "Strange things are afoot at the Circle K"