DNSSEC KSK-2010 Trust Anchor Signal Analysis

MAPRG @ IETF102

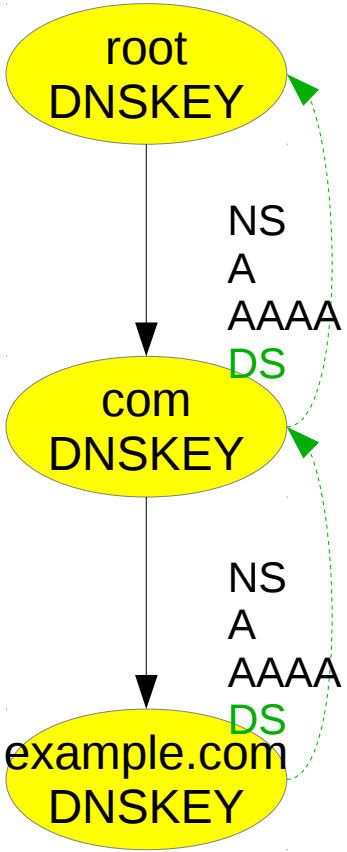
Wes Hardaker
<hardaker@isi.edu>

Overview

- Background: DNSSEC KSK rollover and plan
- Problems with the KSK rollover
- Case study analysis: difficulty in identifying old Trust Anchors
- Measuring the impact of success
- Lessons Learned

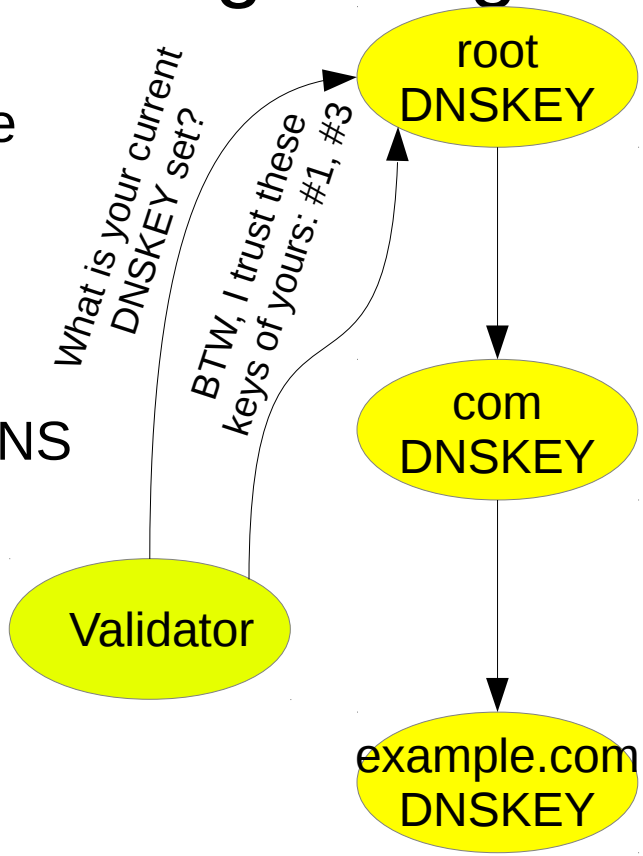
Background: DNSSEC Validation

- DNSSEC validation starts at the top of the tree
  - Requires a bootstrapping Trust Anchor (TA) for the top
  - Chains data integrity downward
- In the end, proof that "www.example.com/A":
  - Exists or doesn't
  - Was not not modified since its signed publication
- But... this only works if you have the root's key as a TA



Background: DNSSEC Trust Anchor Signalling

- Millions of DNS resolvers, some percentage validate
  - They all have a configured TA set
- How do DNSKEY publishers know its safe to roll?
  - DNSSEC at the root is using a flag-day change
- RFC8145 - “Signaling Trust Anchor Knowledge in DNS Security Extensions”
  - Validators signal zones with the TAs they are using
  - They send special queries with trusted key tags
  - “_ta-4a5c-4f66”, type NULL

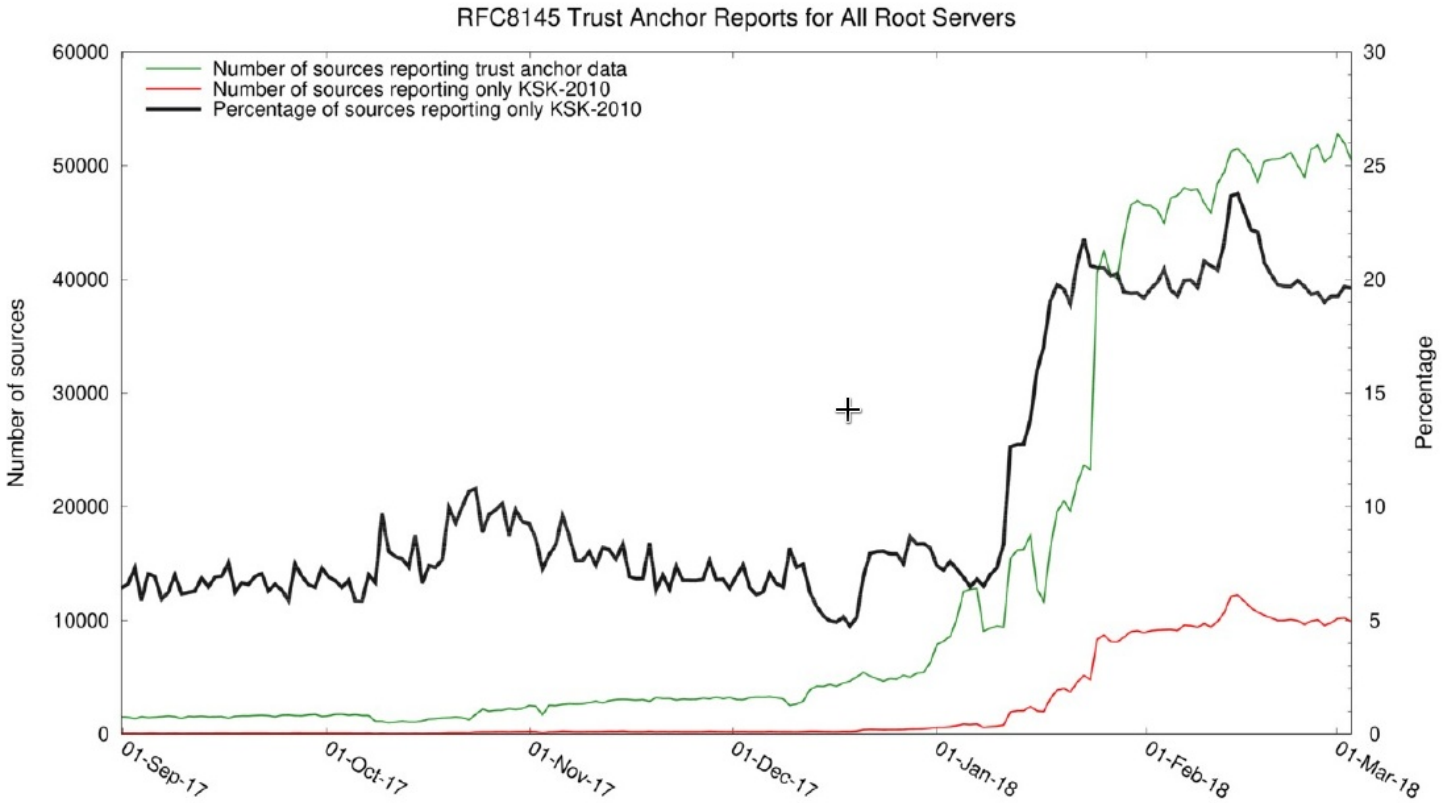


KSK-2010 → KSK-2017 timeline

- ICANN's "DNSSEC Practice Statement" said they would roll the root key after 5 years
- In 2016, this process was started

Date	Event
2016-10-27	New KSK-2017 generated
2017-07-11	KSK-2017 published
2017-10-11	KSK-2017 expected to begin signing
2017-09-27	ICANN (wisely) stopped the rollover plan
2018-10-11	Next expected operational switchover

RFC8145 Measurements of DNSSEC KSK Trust



Graph from ICANN's presentation at DNS-OARC-28

Black Line:

- % of KSK-2010 trust
- **BAD**

Question

- Why are so many **new addresses** regularly appearing sending RFC8145 signals indicating **only trust in KSK-2010?**
- Can data analysis reveal a reason?
- Data analyzed:

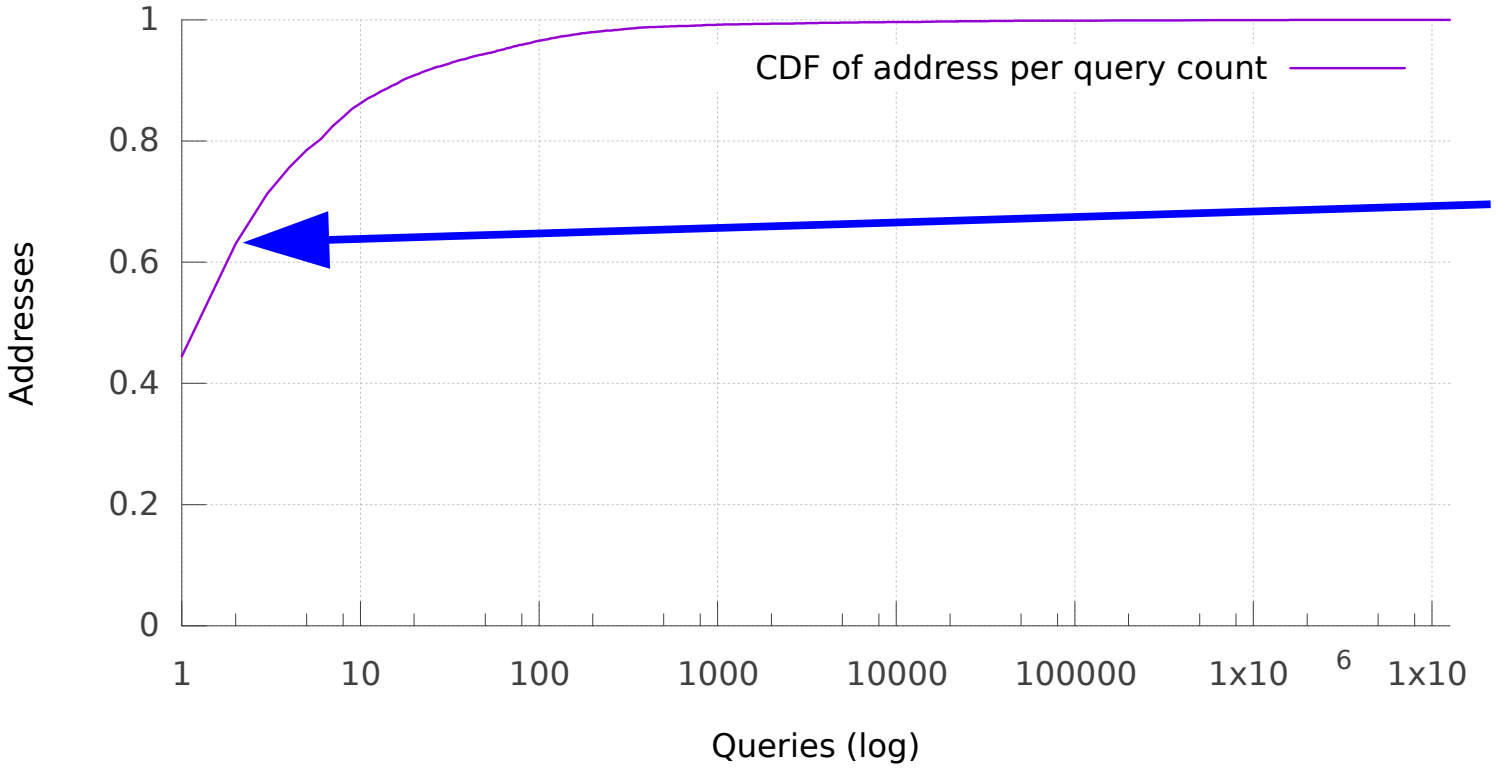
	Pkt Count	Size	Dates
ICANN RFC8145	20.8 M	1.1 GB	2018-01-01 - 2018-03-29
B-Root DNS Requests	83.52 B	2.84 TB	2018-03-01 - 2018-03-29

Reducing the Problem Space

	Description	Count
A	Unique TA signaling sources	1,206,840
B	**A** sources signaling **KSK-2010**	508,533
C	**B** sources sending **only one signal**	310,839
D	**A** sources sending queries to B-Root in March	309,140
E	**D** sources signaling only KSK-2010	113,457
F	**E** sources sending **only one signal**	16,403
G	**F** sources sending only **2-9 other queries**	6702

Summary: **6702 unique addresses** sent a single RFC8145 query to any root in Q1 of 2018 and sent that **single KSK-2010 signal to B-Root** in March and sent **only 2-9 other DNS requests**. *What would cause this strange behavior????*

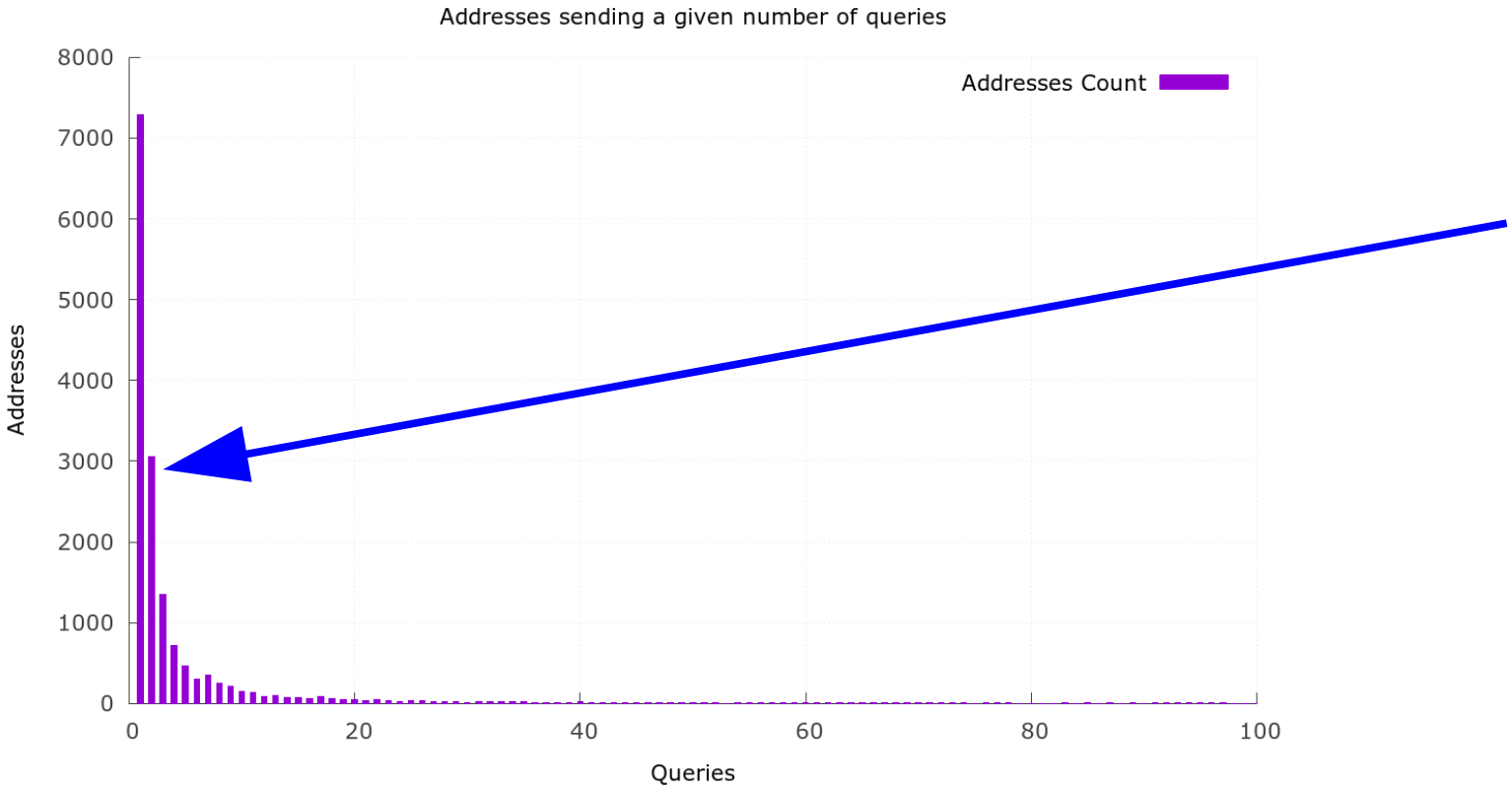
Addresses Sending Specific Query Numbers



63% of the sources sent two or less DNS Queries.

In a month!!!

Addresses Sending Specific Query Numbers



63% of the sources sent two or less DNS Queries.

In a month!!!

Is There Commonality?

- Given:
  - All the DNS requests to B-Root
  - From these addresses
  - During March
- Can we find a commonality in **other DNS Query names** sent?

Extracting the Top Common Domains Queried

The top Query names from 6702 sources sending 2-9 queries

Query Name	Count
_ta-4a5c (The KSK-2010 TA signal)	15447
“.” (Root zone label)	9182
VPN-PROVIDER.com	3156
VPN-PROVIDER-ALTERNATE.com	415
_sip._udp.ANOTHER-DOMAIN.com	86

Clearly a large number of requests are from **VPN-PROVIDER users**

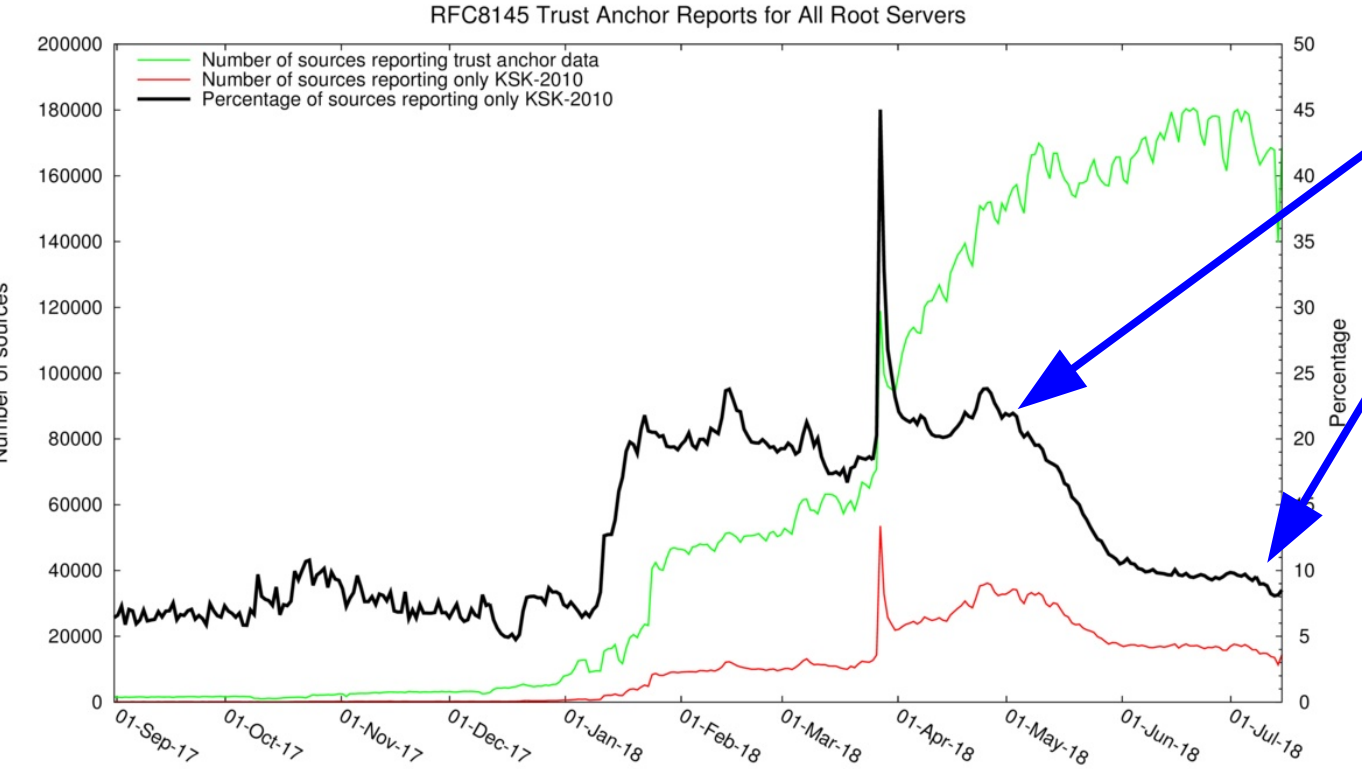
Examining the VPN-PROVIDER software

- Downloading the Android version of the software...
- String searching all files for “49AAC11D7B6F64...”
  - SHA256 fingerprint of the KSK-2010 key
  - Revealed a “root.key” file containing only the KSK-2010 key
- Other packaged files:
  - *libdnssec.so*
  - Shared library distributed from the Unbound DNSSEC resolver

Contacting the Vendor

- I reached out to the vendor
  - Thanks to ICANN OCTO staff finding contact information quickly
- The vendor:
  - Agreed it was a problem affecting 10 software packages
  - Promised to release new software in the coming months

Impact of This Effort



First VPN software update released

Android software released

IOS this week?

That was hard. Were there other studies?

- Warren Kumari
  - Searched for the keys in GitHub's search interface

	KSK-2010	KSK-2017
GitHub	2069	412
Google	1390	728

- Roy Arends
  - Analyzing some of these results for forking, popularity, etc

Lessons Learned

- Flag day Trust Anchor rollovers are hard
- Tracking down misuse in 1,000,000+ sources is hard
- I solved a small slice of the pie
  - These were all 1 user between each address
  - What about the resolvers signaling from a large ISP?
  -
- Why are rolling TAs for DNSSEC so hard?

Protocol Design Recommendations: Signaling

- Why is RFC8145 such a poor TA signaling mechanism?
  - The signal is decoupled from other requests
    - (The signal can go to one destination, requests for keys to another)
    - Two validators behind a NAT or DNS forwarder confuse analysis
  - The signal does not include an intent to validate
- Signals need:
  - To be tied to requests for the keys themselves
  - To include an intent to use the results (or not)

Protocol Design Recommendations: Rollovers

- Design for automatic updates for trust anchor rollovers
  - During initial protocol design!
  - Afterward is challenging
- Select update frequency choices wisely
  - Annually: get everyone's software working or else!
  - Rarely: assume its hard and things will break
    - Use strong, well protected keys

Questions?