Effects of KSK Roll over

Oops, so what now?

Jaap Akkerhuis
just a messenger

NLnet Labs

What we wanted

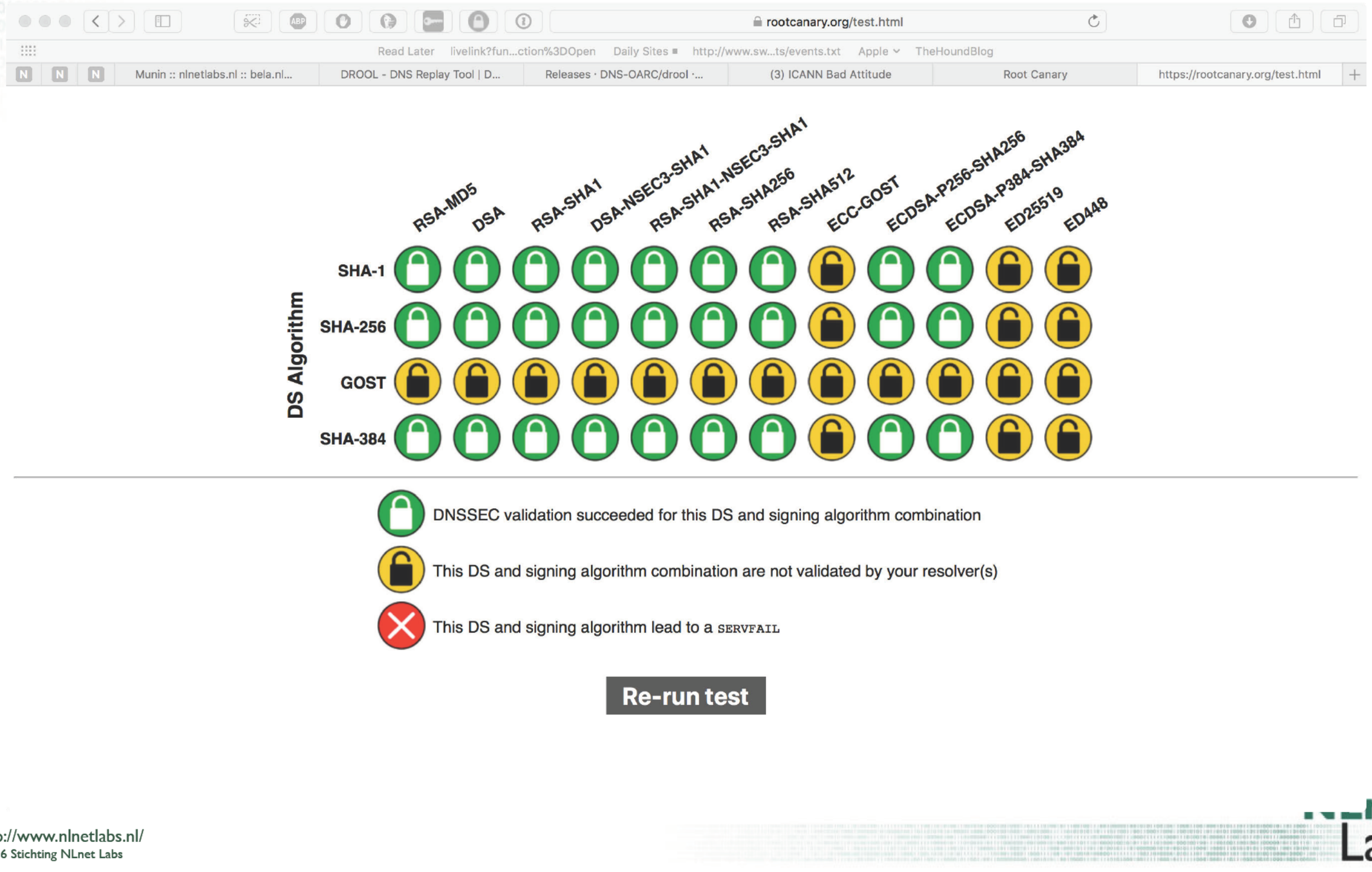
- Report about effects of the KSK roll
  - Supported algorithms
  - Packet size
  - To gather knowledge
- Will report about mechanism

Ripe DNS Atlas Hackathon 2017

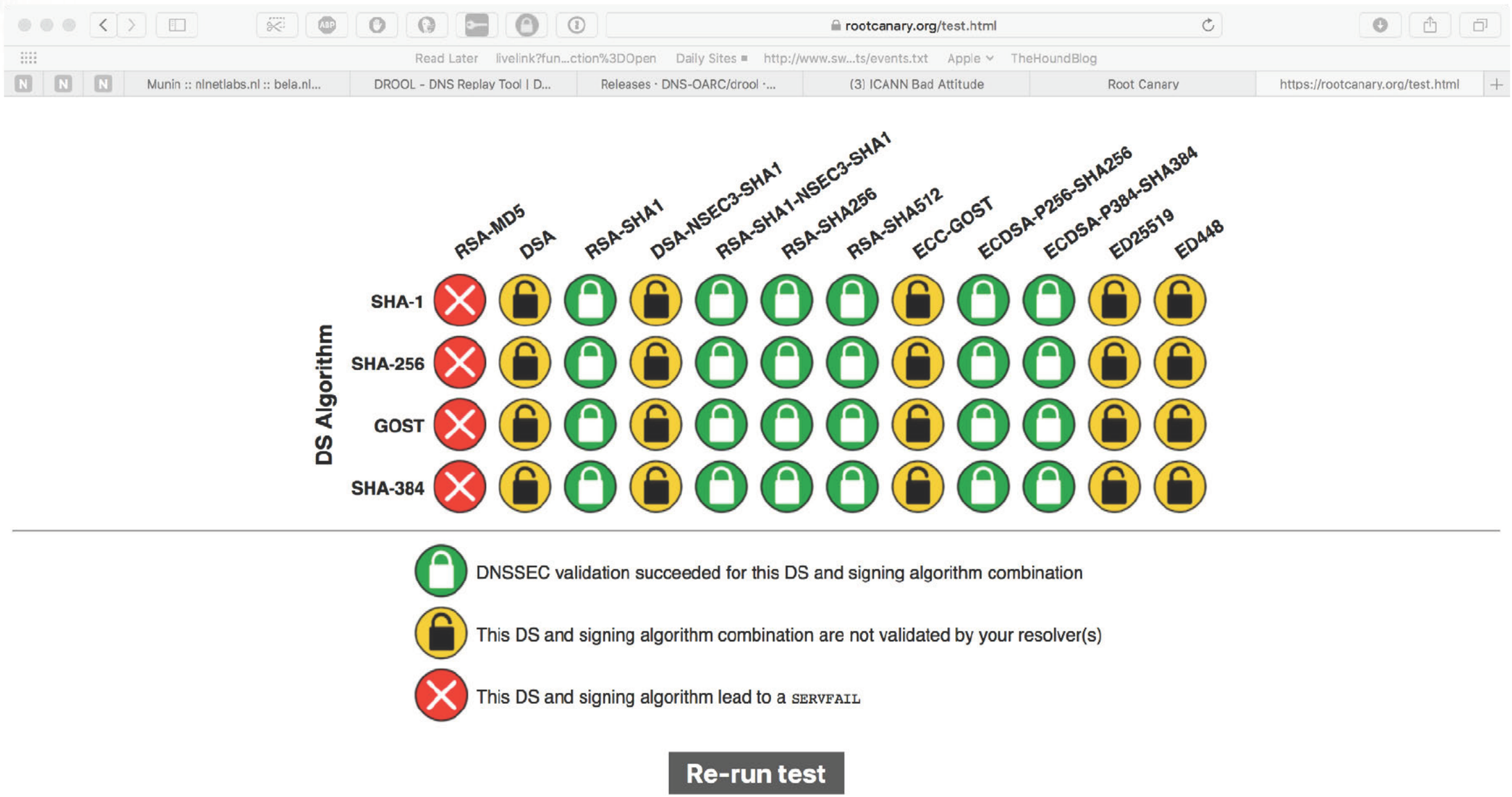
- Test which probes see DNSSEC
- What Algorithms are supported
- Test against various name servers
- Display in a nice way

NLnet Labs

ICANN-60 NS servers

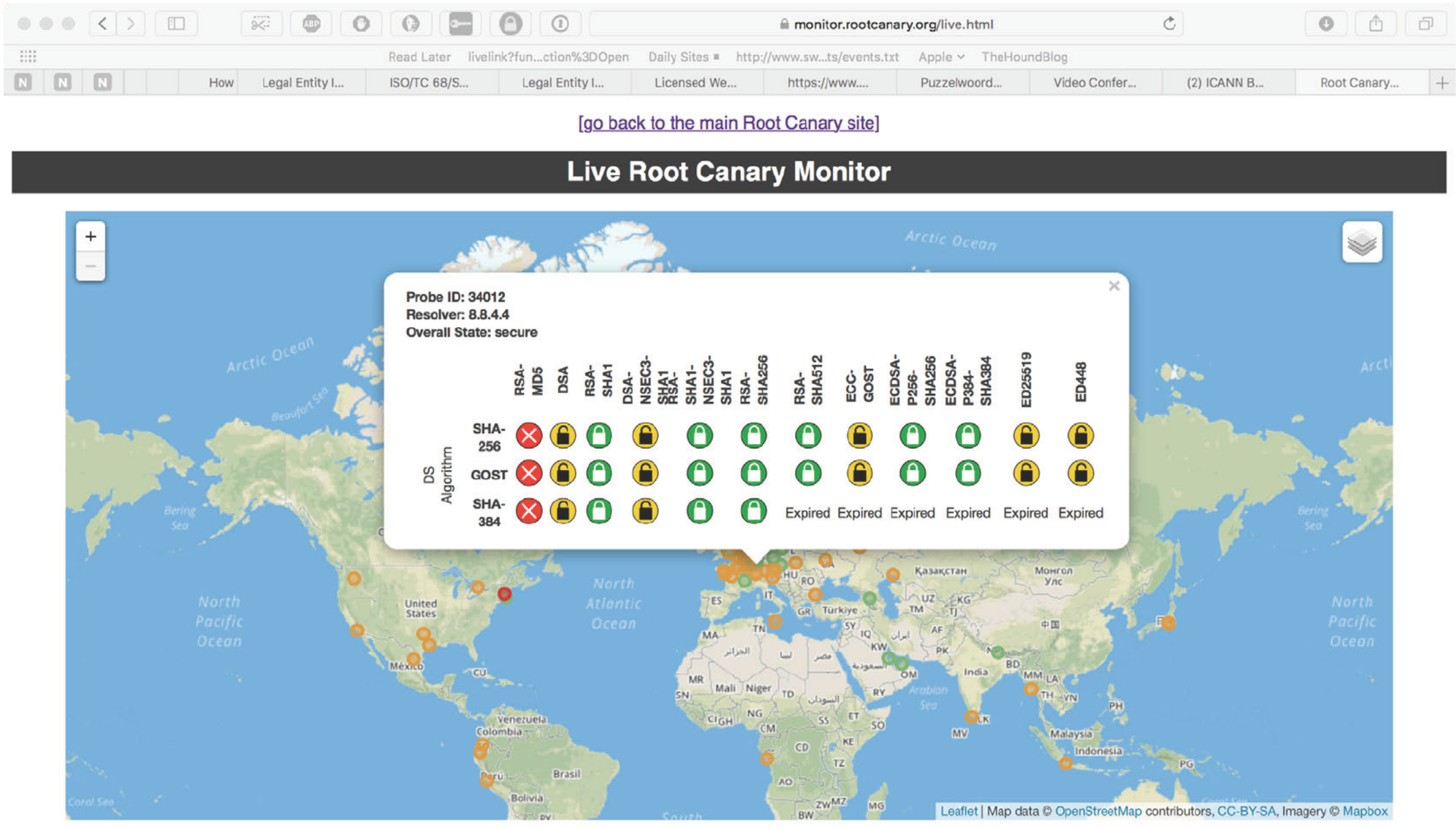


Google



NLnet Labs

Continue measurements



Root Canary was born

The Root Canary

Quantifying the Quality of DNSSEC Validation in the Wild

SIDN LABS

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ICANN

NLnet Labs

SURF NET

Northeastern University

UNIVERSITY OF TWENTE.

http://www.nlnetlabs.nl/

NLnet Labs

Canary in the virtual coalmine

(Now stealing slides from Moritz)

- Goals:
  - **Track operational impact** of the root KSK rollover, act as a warning signal that validating resolvers are failing to validate with the new key
  - **Measure validation during** the **KSK rollover** from a global perspective **to learn from this type of event**

Canary in the virtual coalmine

- Goals:
  - **Track operational impact** of the root KSK rollover, act as a warning signal that validating resolvers are failing to validate with the new key
  - **Measure validation during** the **KSK rollover** from a global perspective **to learn from this type of event**

Measurement methodology

- Use four perspectives:
  - Online perspectives:
    - RIPE Atlas
    - Luminati
    - APNIC DNSSEC measurement
      (current thinking: use data during evaluation)
  - “Offline” perspective (analysed after measuring)
    - Traffic to root name servers (multiple letters)

Measurement methodology

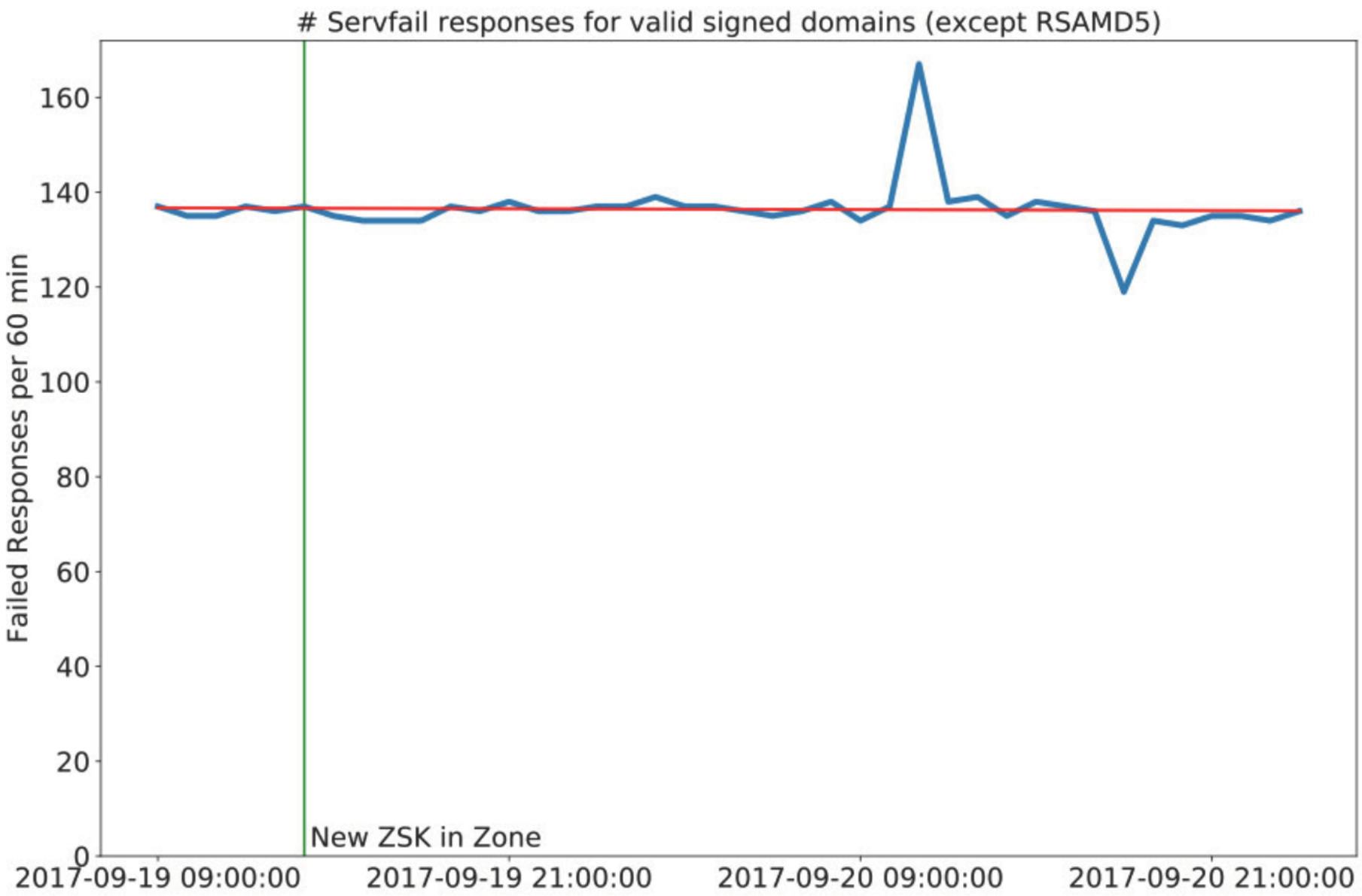
- **Luminati:** HTTP(s) proxy service

- 2.3 Million exit nodes - usually of residential users
    - Allows us to send HTTP(s) traffic via a central Luminati server through the exit nodes
    - This HTTP request triggers a DNS query
- Covers > 15,000 ASes
- Of which > 14,000 are not covered by RIPE Atlas

Canary in the virtual coalmine

- Preliminary Findings after 2017-09-19:

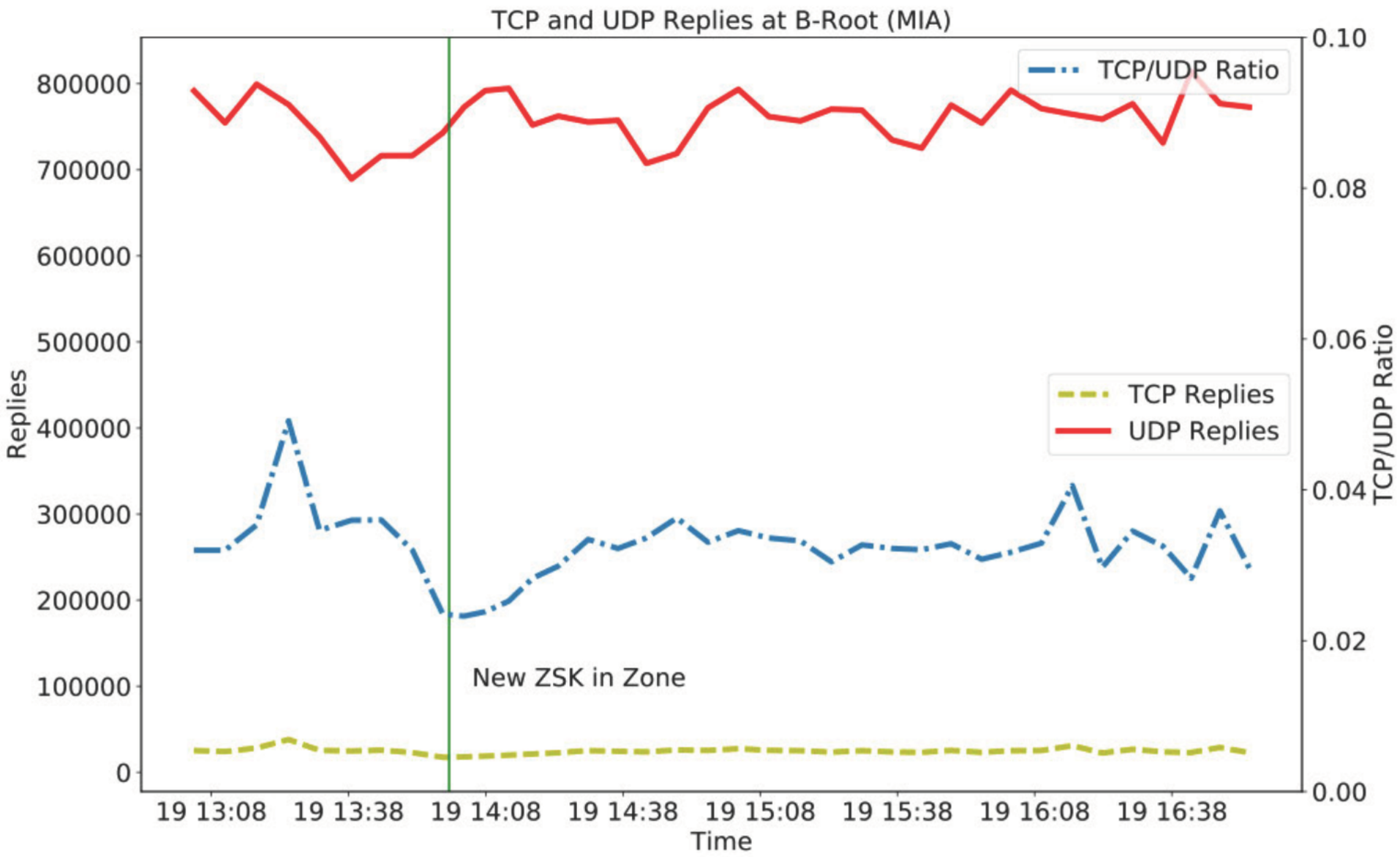
RIPE NCC
RIPE Atlas



https://rootcanary.org/

Canary in the virtual coalmine

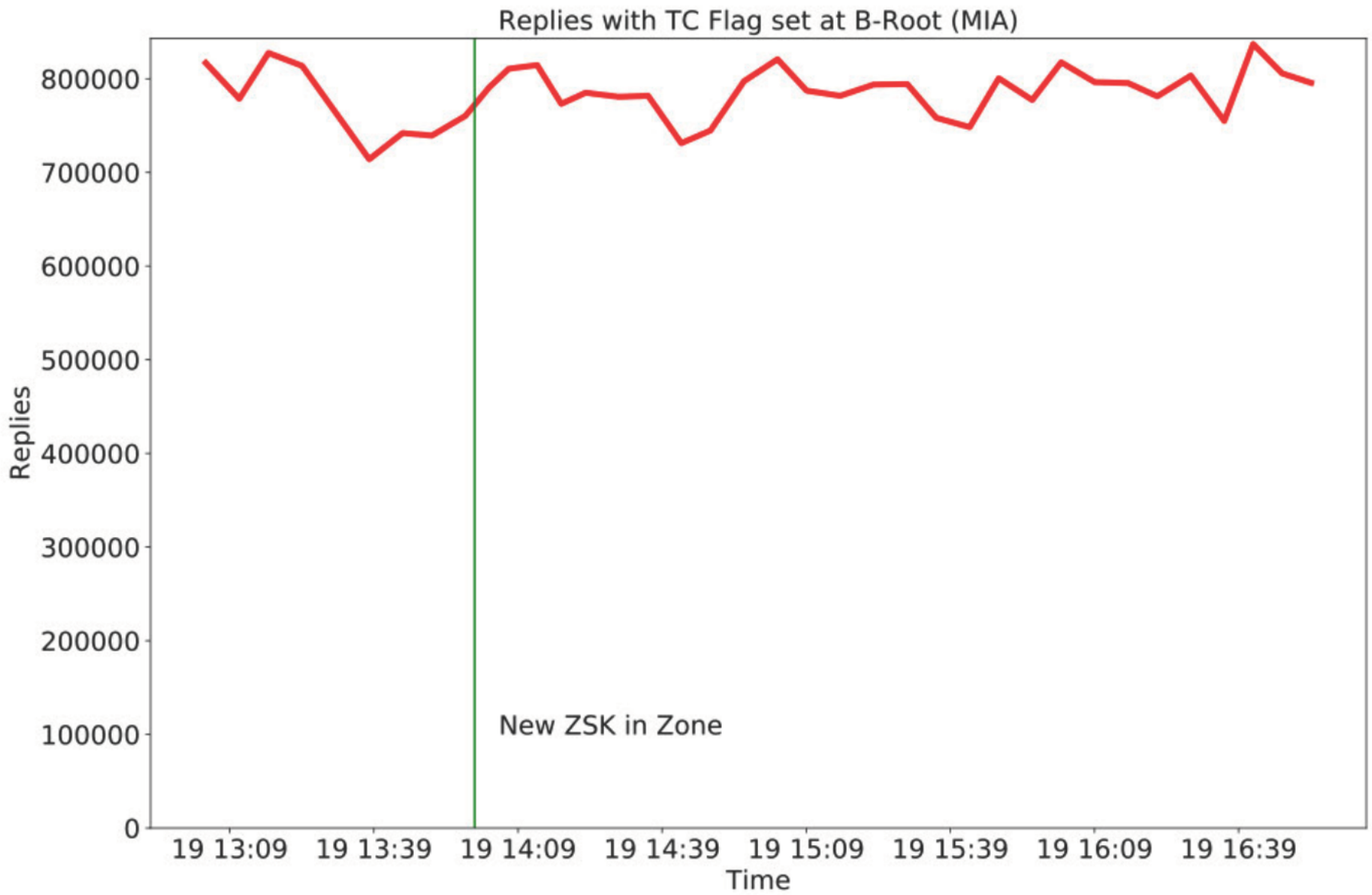
- Preliminary Findings after 2017-09-19: Root



https://rootcanary.org/

Canary in the virtual coalmine

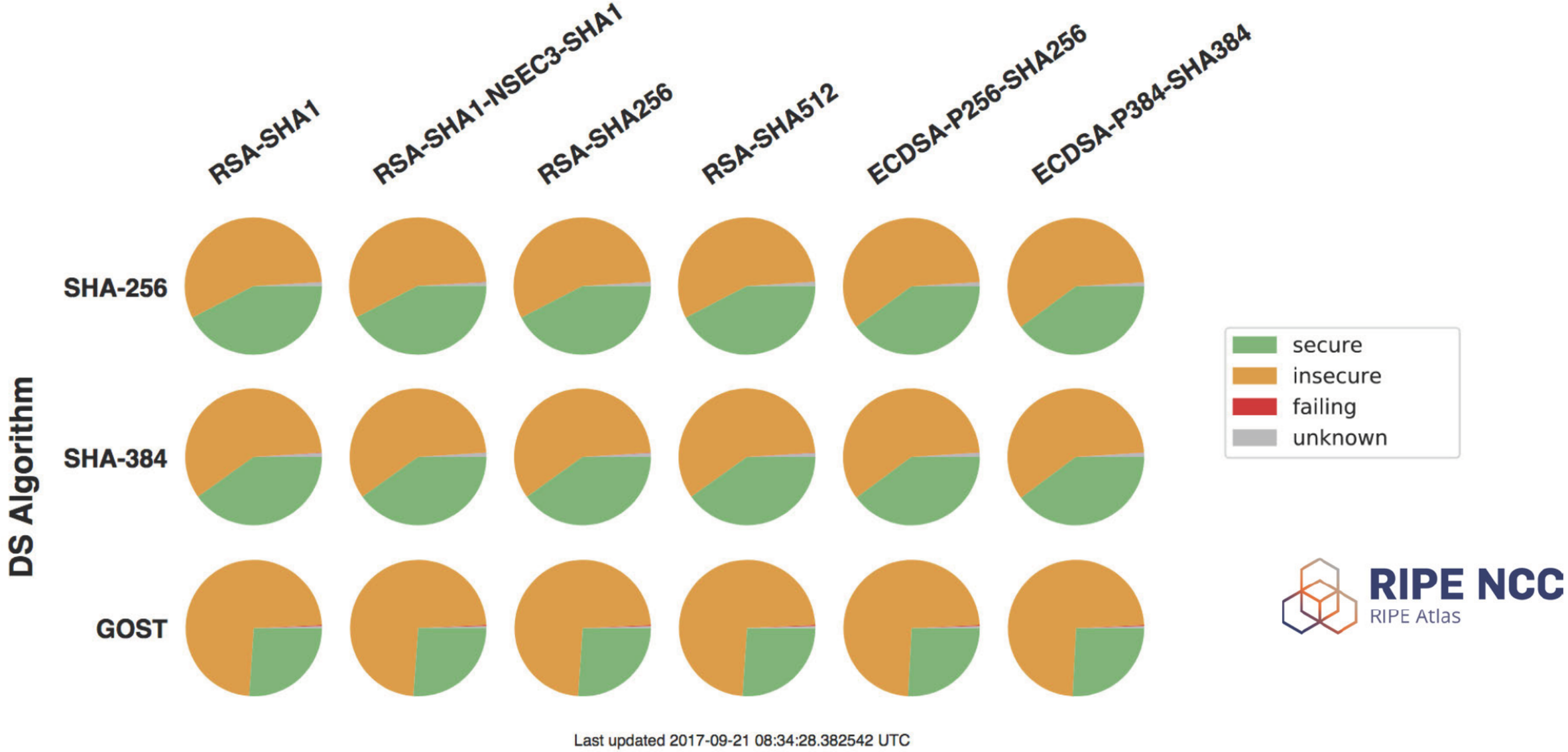
- Preliminary Findings after 2017-09-19: Root



https://rootcanary.org/

Algorithm Support

- For common signing algorithms:

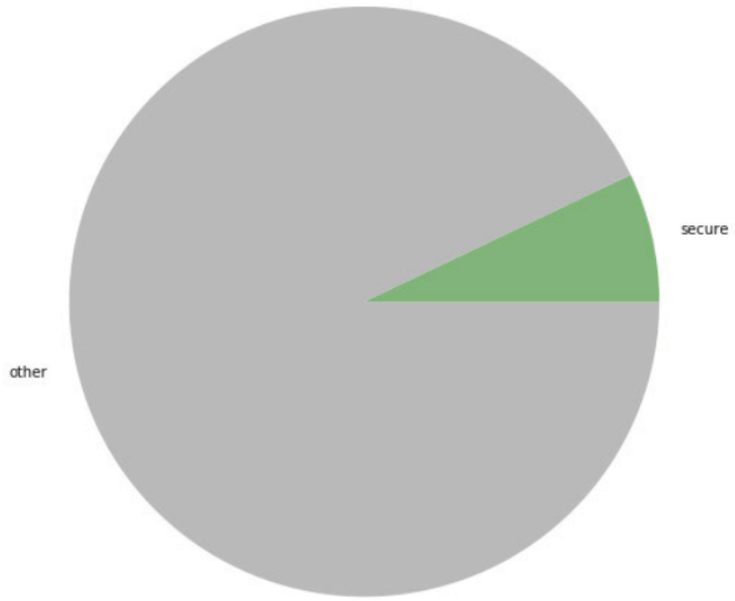


https://rootcanary.org/

Algorithm Support

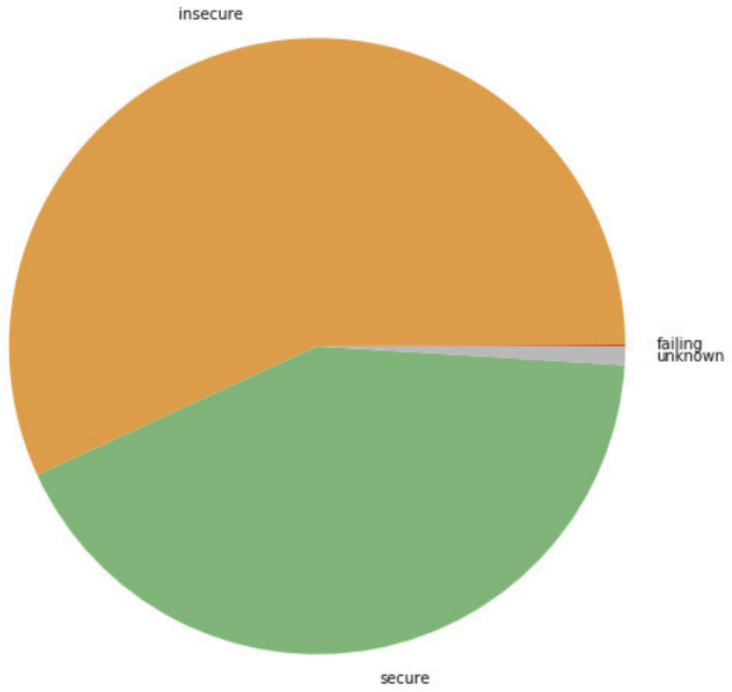
- Luminati vs RIPE Atlas: SHA256-RSA-SHA1

Luminati



- ~ 13,000 VPs
- 7% validating

RIPE NCC
RIPE Atlas



- ~ 9,000 VPs
- 42% validating

https://rootcanary.org/

Fingerprinting Resolvers

- 1319 VPs
- Google Public DNS

DS Algorithms	RSA-MD5	DSA	RSA-SHA1	DSA-NSEC3-SHA1	RSA-SHA1-NSEC3-SHA1	RSA-SHA256	RSA-SHA512	ECC-GOST	ECDSA-P256-SHA256	ECDSA-P384-SHA384	ED25519	ED448
SHA-256	✗	🔓	🔒	🔓	🔒	🔒	🔒	🔓	🔒	🔒	🔓	🔓
GOST	✗	🔓	🔒	🔓	🔒	🔒	🔒	🔓	🔒	🔒	🔓	🔓
SHA-384	✗	🔓	🔒	🔓	🔒	🔒	🔒	🔓	🔒	🔒	🔓	🔓

https://rootcanary.org/

Fingerprinting Resolvers

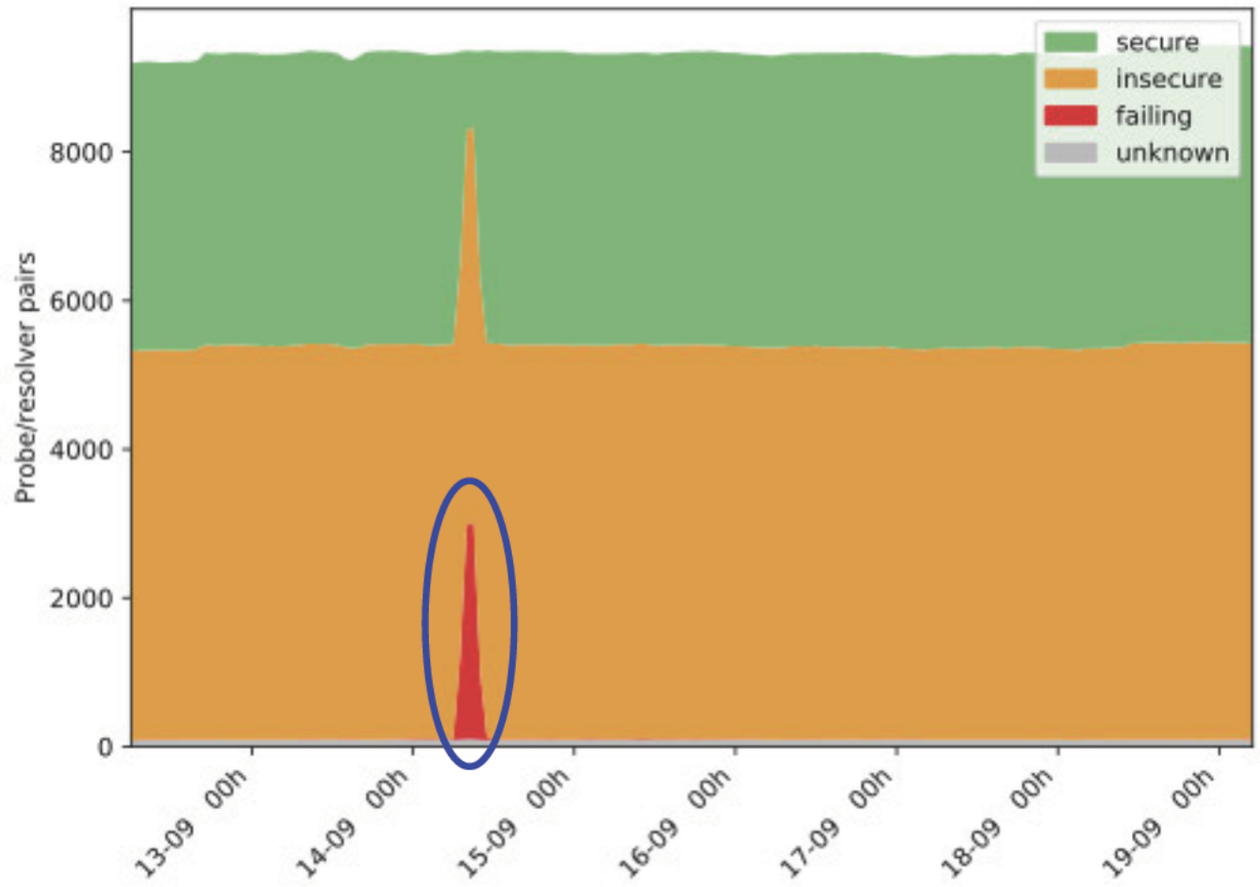
- 19 VPs
- PowerDNS Recursor or Knot Resolver

DS Algorithms	RSA-MD5	DSA	RSA-SHA1	DSA-NSEC3-SHA1	RSA-SHA1-NSEC3-SHA1	RSA-SHA256	RSA-SHA512	ECC-GOST	ECDSA-P256-SHA256	ECDSA-P384-SHA384	ED25519	ED448
SHA-256	✗	🔒	🔒	🔒	🔒	🔒	🔒	✗	🔓	🔓	✗	✗
GOST	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
SHA-384	✗	🔒	🔒	🔒	🔒	🔒	🔒	✗	🔓	🔓	✗	✗

https://rootcanary.org/

Serving Stale Data?

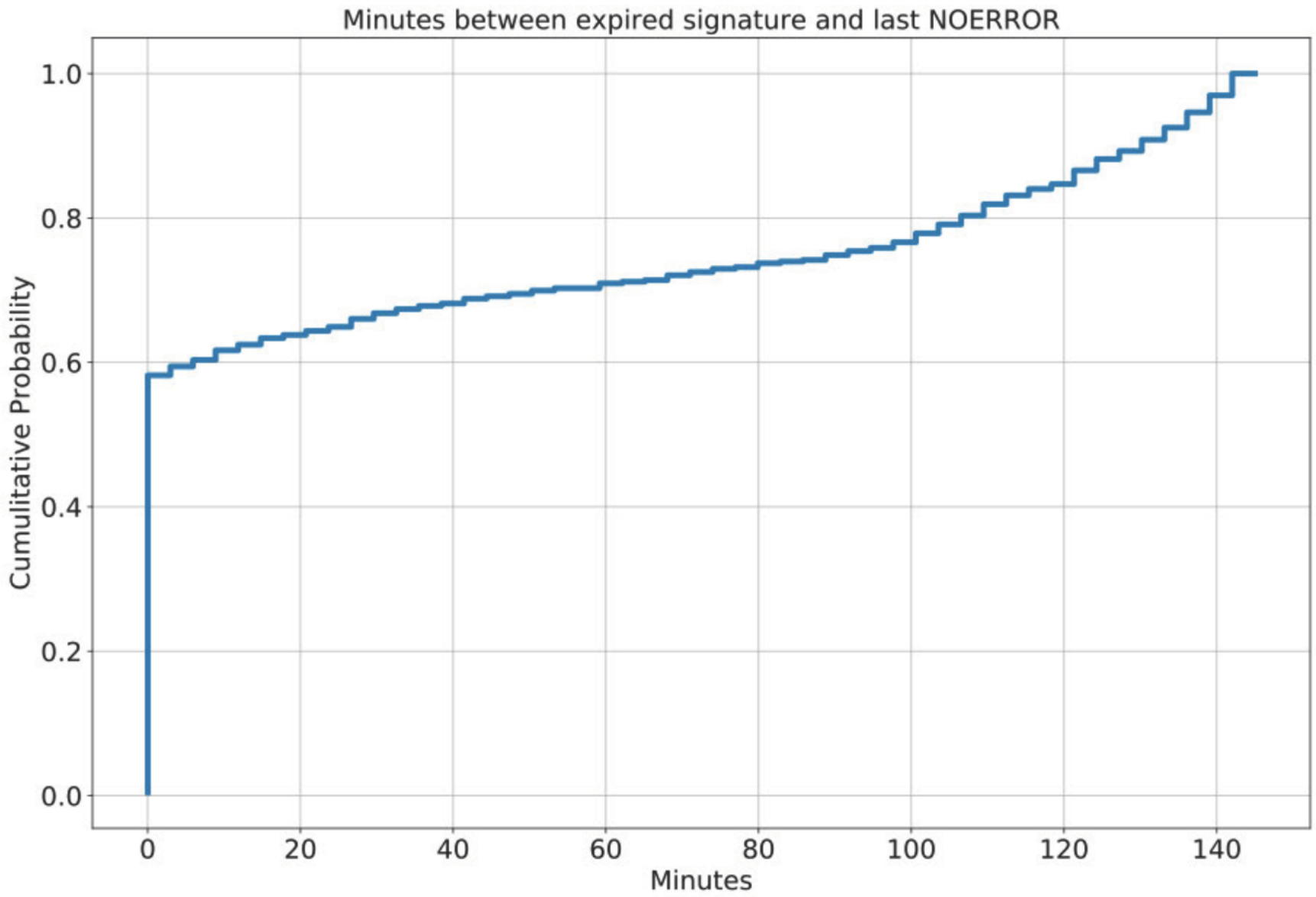
- We've messed up automatic resigning



RIPE NCC
RIPE Atlas

https://rootcanary.org/

Serving Stale Data?



https://rootcanary.org/

Serving Stale Data?

- 552 resolvers keep validating, among
  - 25 of 280 IPs from Google's Public DNS
  - 29 out of 32 from French ISP Free SAS
    - 9 out of 10 from Dutch ISP XS4ALL
- Future work: How long is their timeout?

You can help!

- Run small shell script that uses *dig* to query our test domains from within your network
  - Using your default resolvers
  - Once every hour
- Please come talk to me if you're interested

Them

Roland van Rijswijk-Deij <r.m.vanrijswijk@utwente.nl>

More info

- Project webpage:
  https://rootcanary.org/

- Online algorithm test:
  https://rootcanary.org/test.html

- Current results for RIPE Atlas-based measurement:
  https://portal.rootcanary.org/rcmstats.html

- Live feed for RIPE Atlas-based measurement:
  https://monitor.rootcanary.org/live.html

While waiting ...

- Twiddling thumbs
- New test might be added

NLnet Labs

Questions?

NLnet Labs

NLnet Labs