# The Root Canary

Quantifying the Quality of DNSSEC Validation in the Wild

# Project partners

UNIVERSITY OF TWENTE.

SURF NET

Northeastern University

NLnet Labs

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ICANN

SIDN LABS

# 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

- We have **signed and bogus** records for **all algorithms** and **most DS algorithms**

- This gives us one of three outcomes:
  - Resolver **validates correctly**
  - Resolver **fails to validate** (SERVFAIL)
  - Resolver **does not validate**
  - (yes, there are **corner cases** probably **not covered** by these three options)

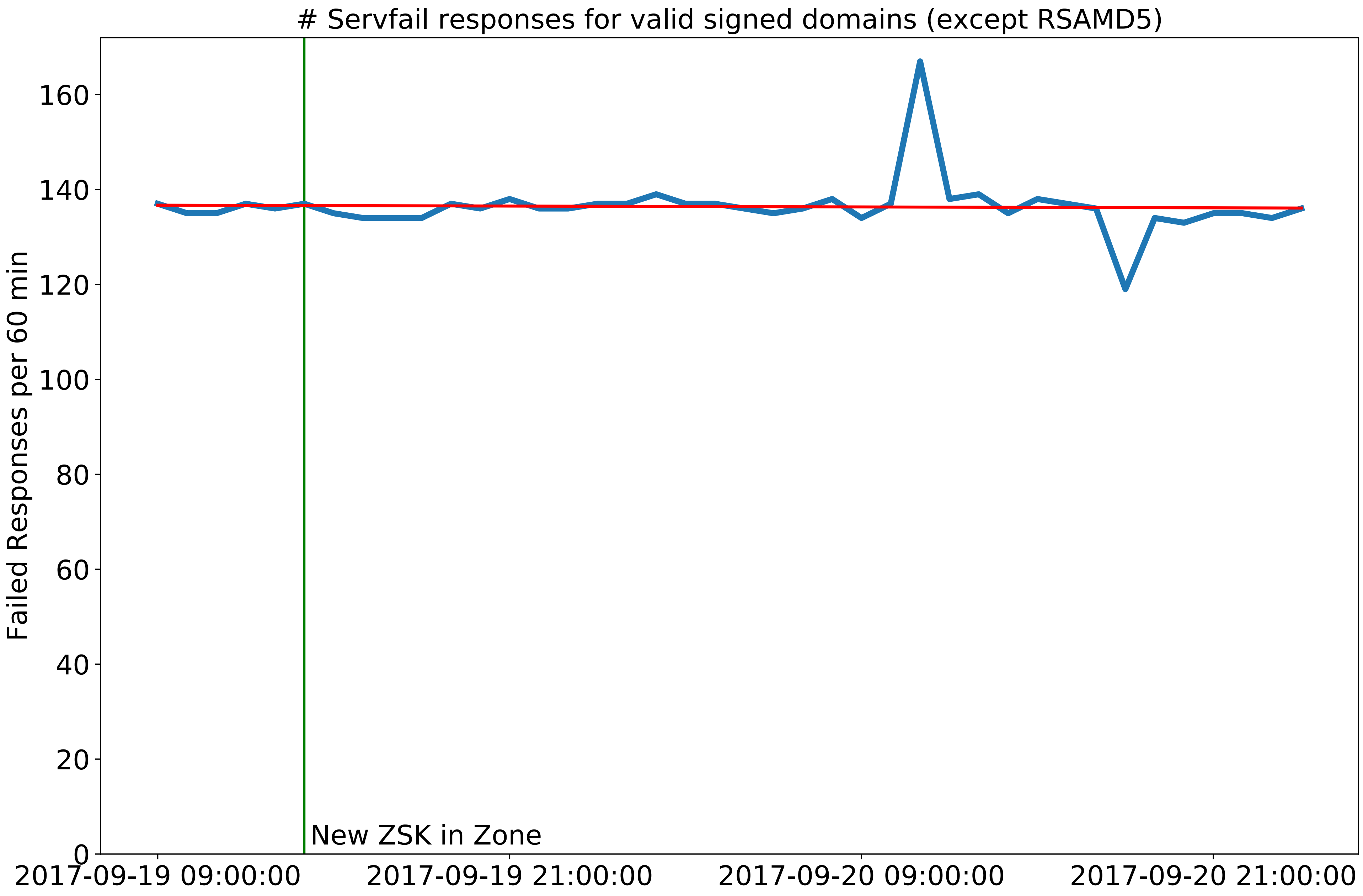
- **Side-effect**: measure support for algorithms

# 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

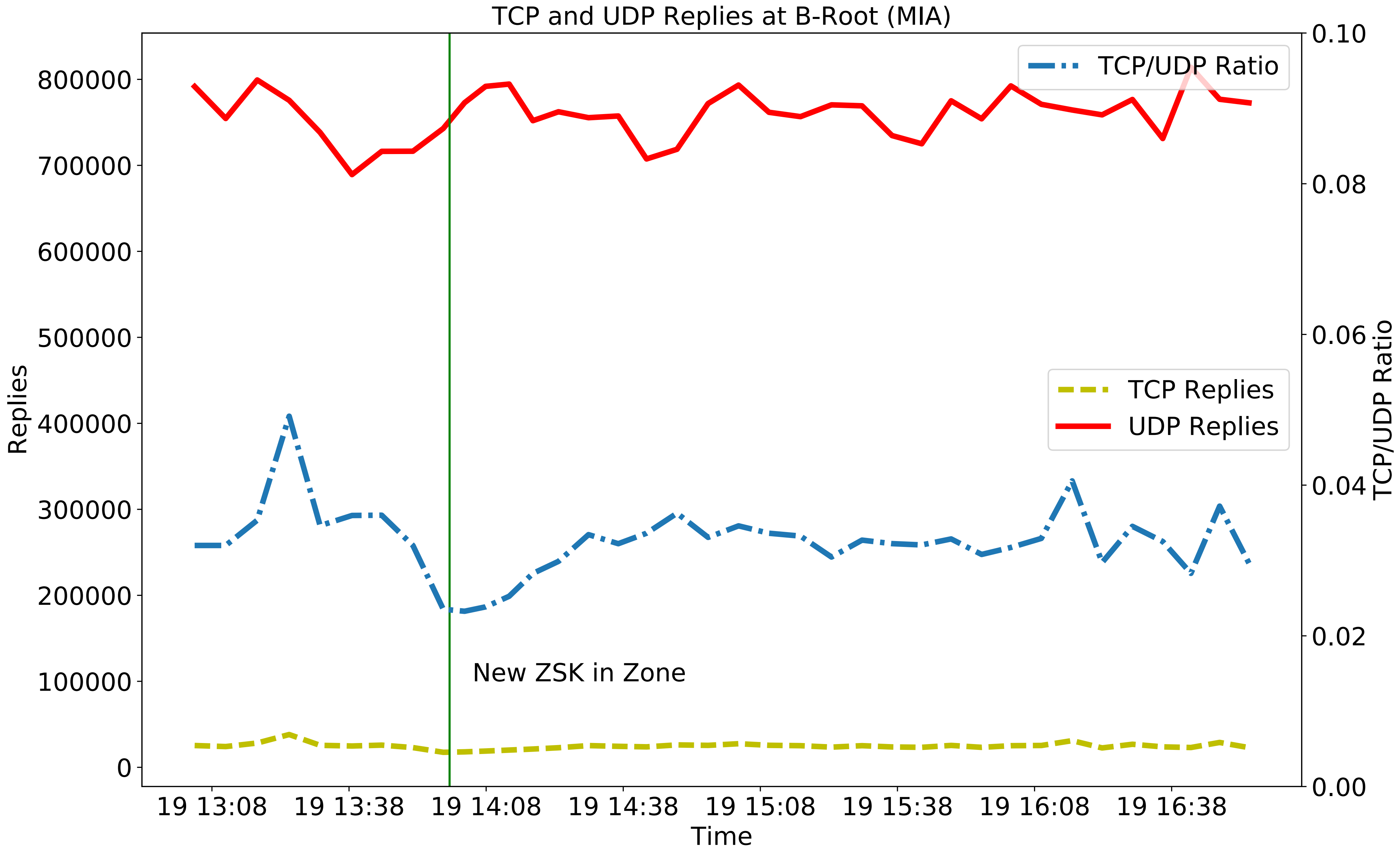
- Preliminary Findings after 2017-09-19:



https://rootcanary.org/

# Canary in the virtual coalmine

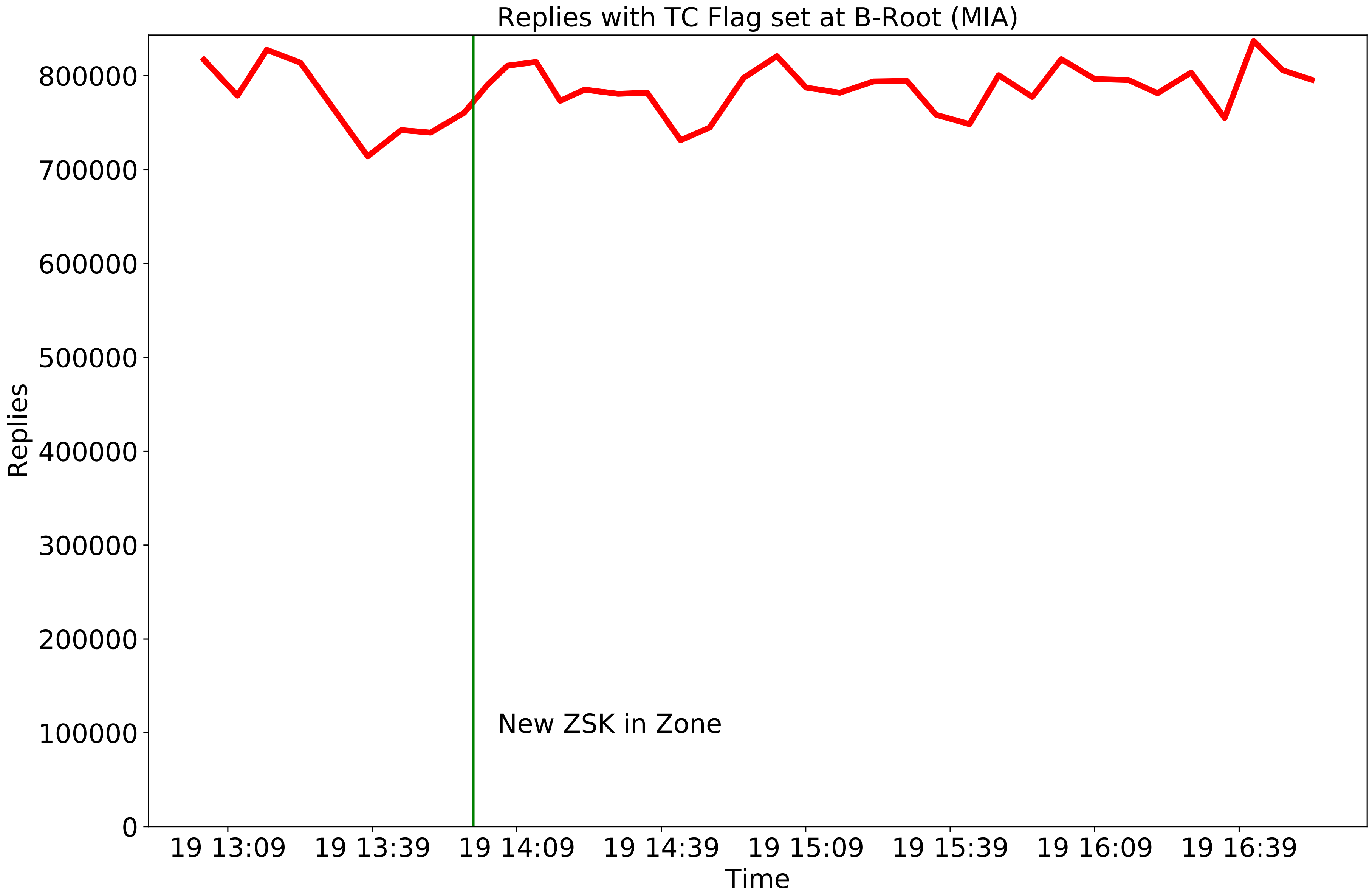
- Preliminary Findings after 2017-09-19: Root



https://rootcanary.org/

# Canary in the virtual coalmine

- Preliminary Findings after 2017-09-19: Root



# Goals
# - beyond the Root KSK Rollover

- **How well** do (validating) resolvers support DNSSEC Algorithms?

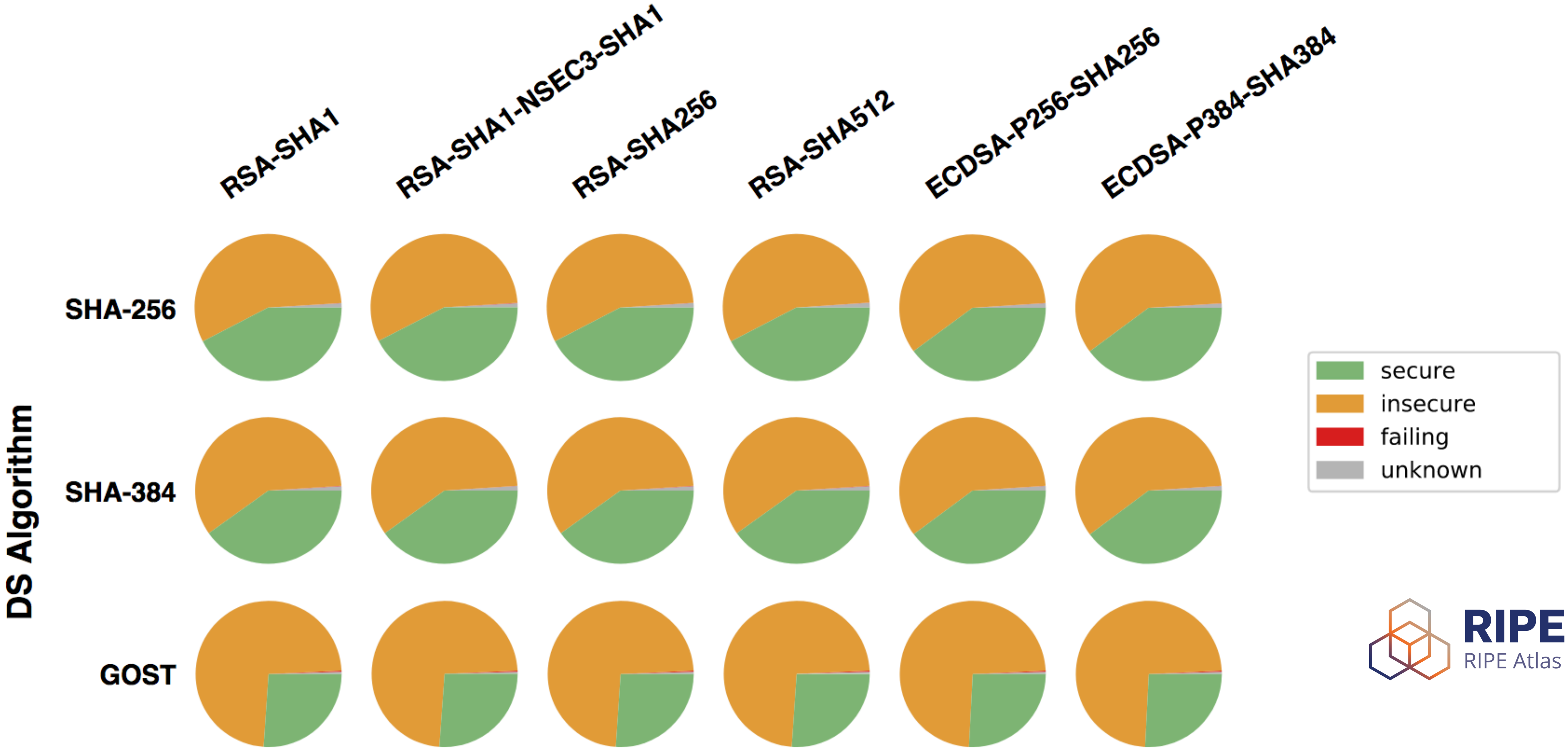
- Can we use those measurements for **fingerprinting** recursive resolvers?

- What happens when signature **expire**?

- Can **YOU** help us to improve our ground truth data?

# Algorithm Support

- For common signing algorithms:



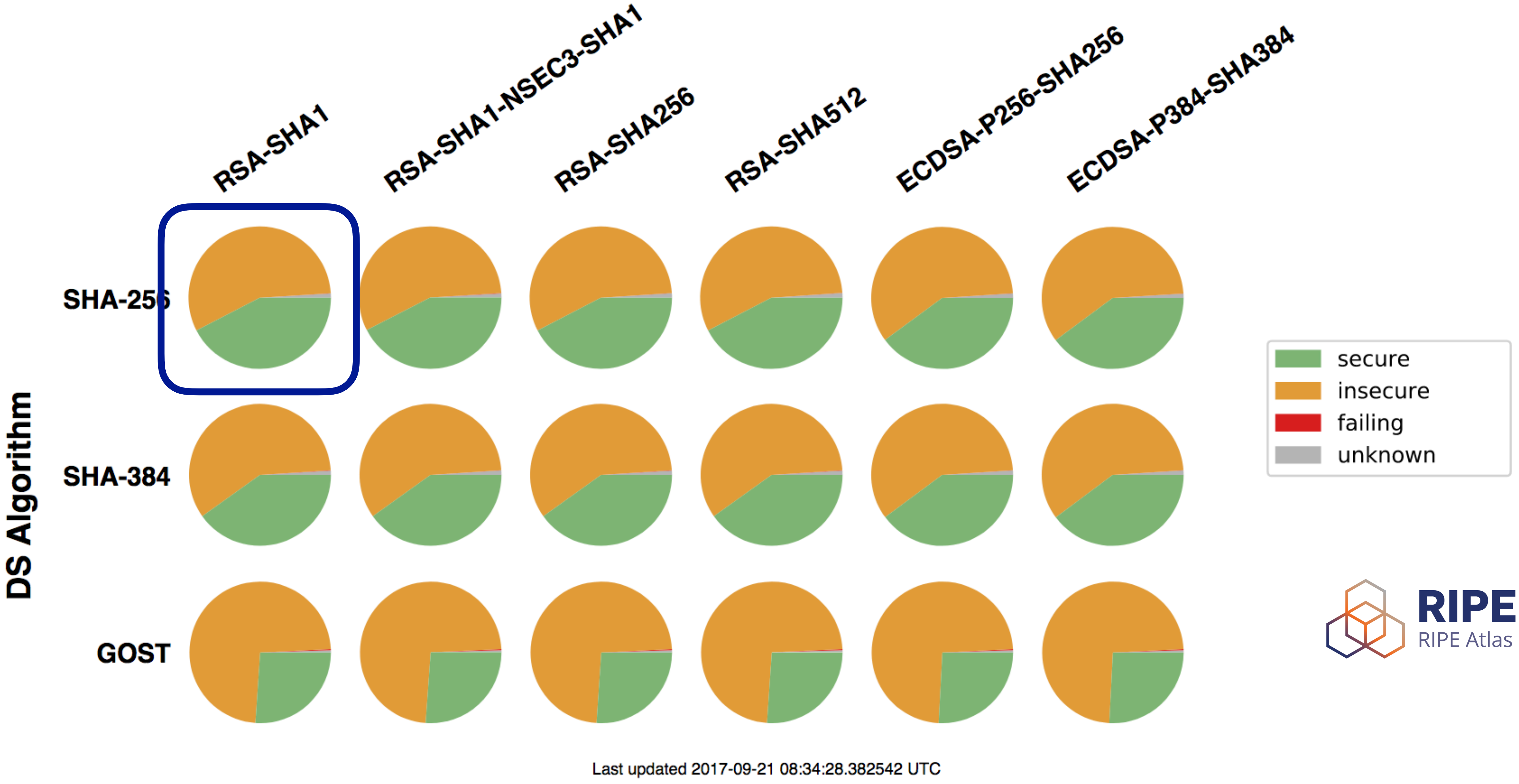
Last updated 2017-09-21 08:34:28.382542 UTC

RIPE NCC
RIPE Atlas

https://rootcanary.org/

# Algorithm Support

- For common signing algorithms:



RIPE NCC
RIPE Atlas

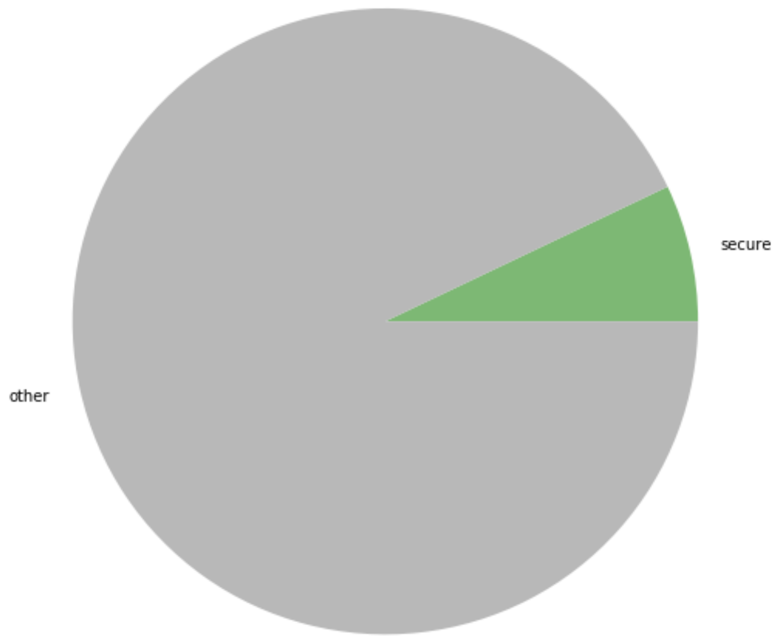
**https://rootcanary.org/**

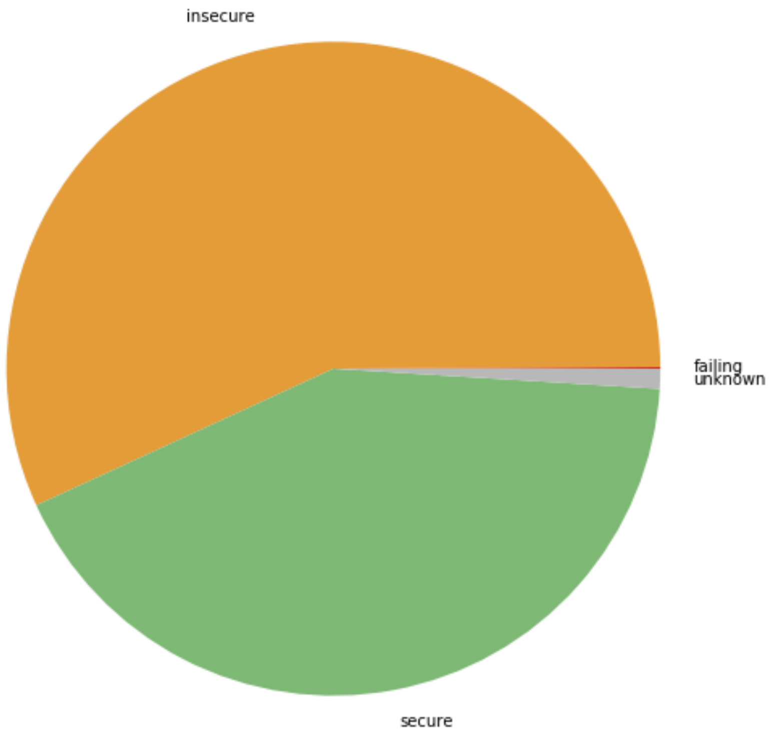
# Algorithm Support

- Luminati vs RIPE Atlas: SHA256-RSA-SHA1

Luminati

RIPE NCC
RIPE Atlas



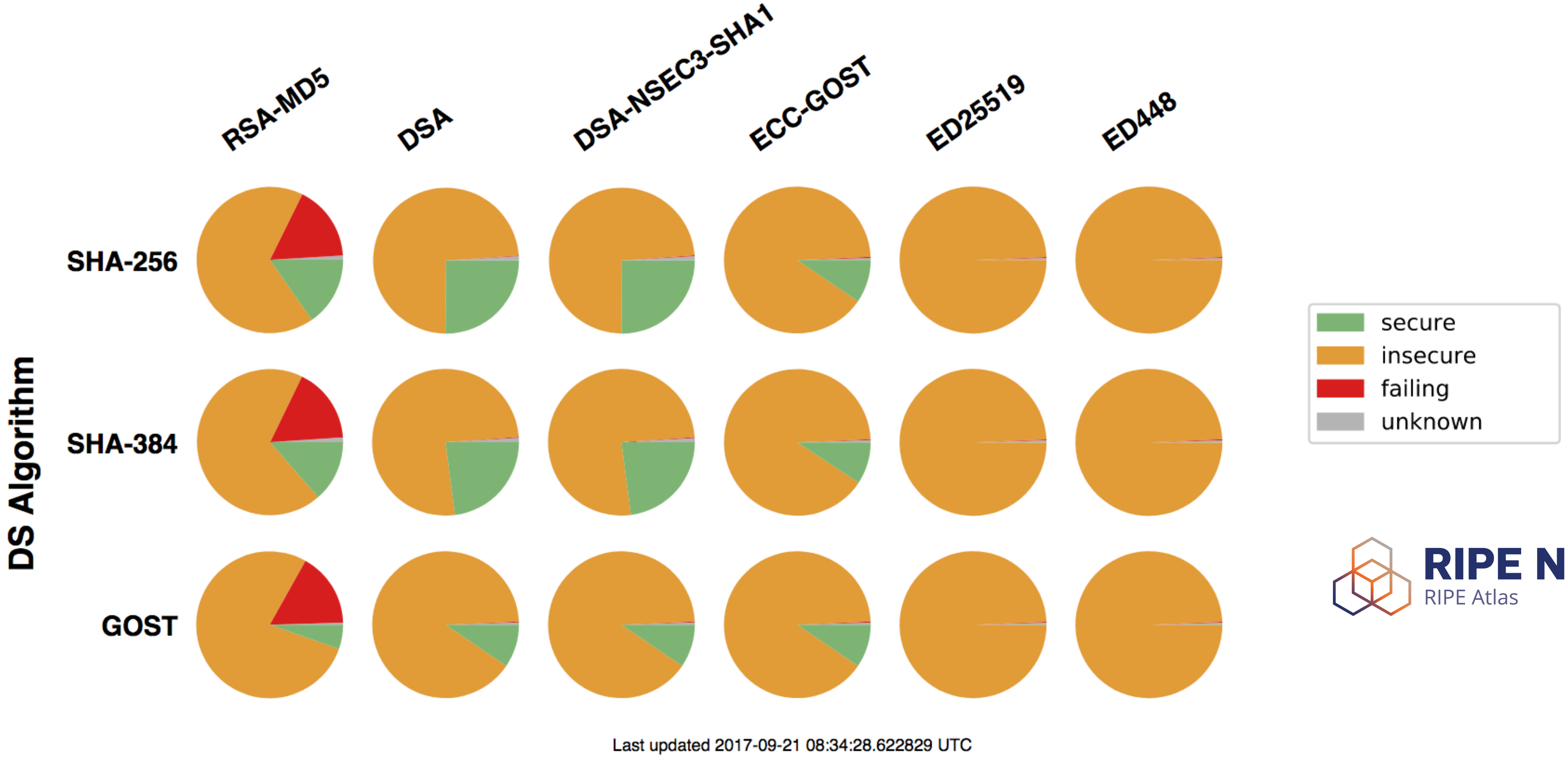


- ~ 13,000 VPs
- 7% validating

- ~ 9,000 VPs
- 42% validating

# Algorithm Support

- For deprecated and brand new algorithms:

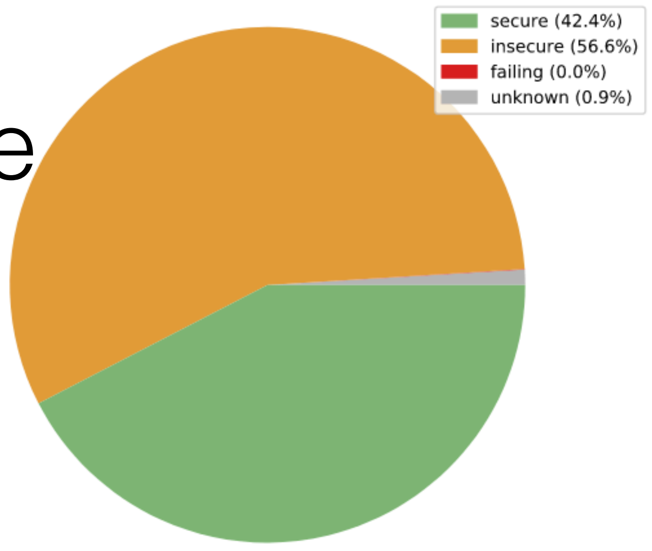


RIPE NCC
RIPE Atlas

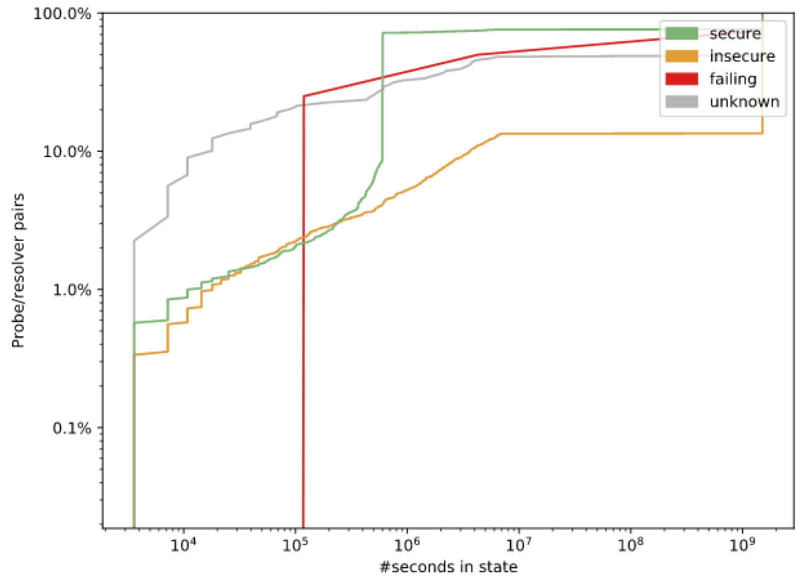
https://rootcanary.org/

# Details

current state of probe population

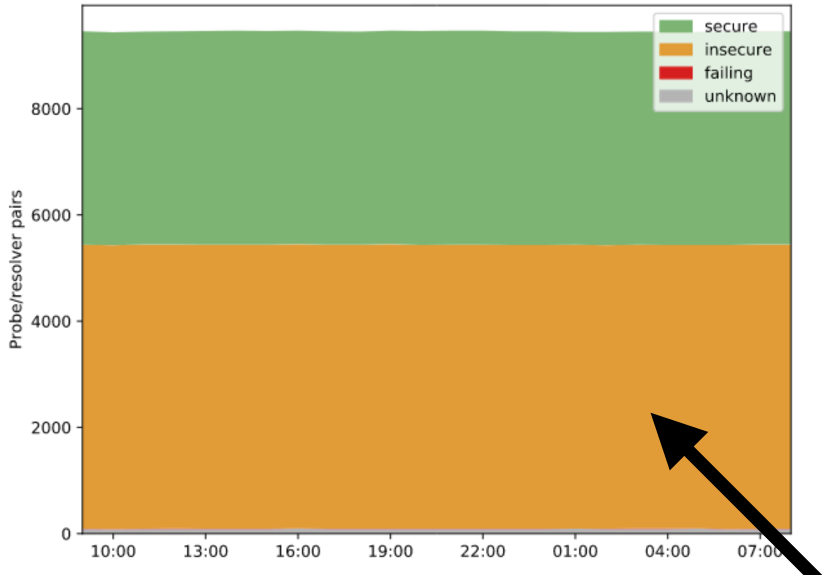


Current probe status for all probes

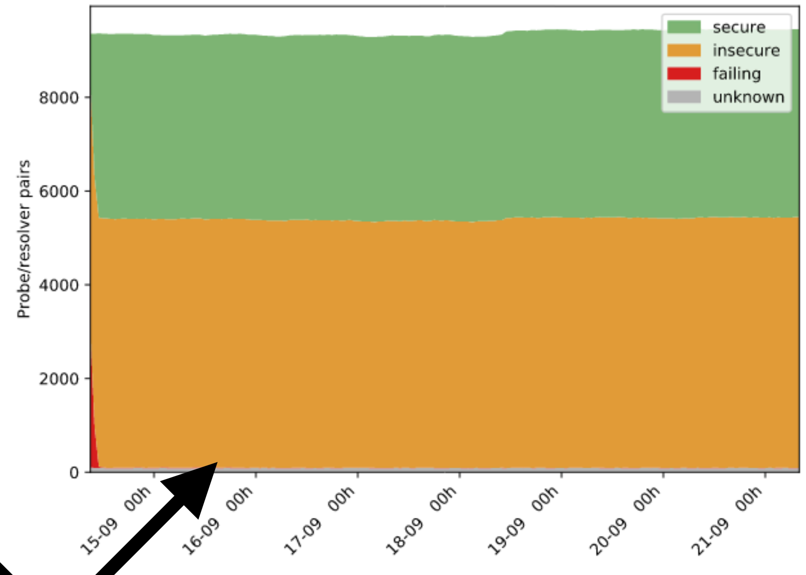


CDF for current time in state

CDF for time probes are in a state (shorter == many state changes)



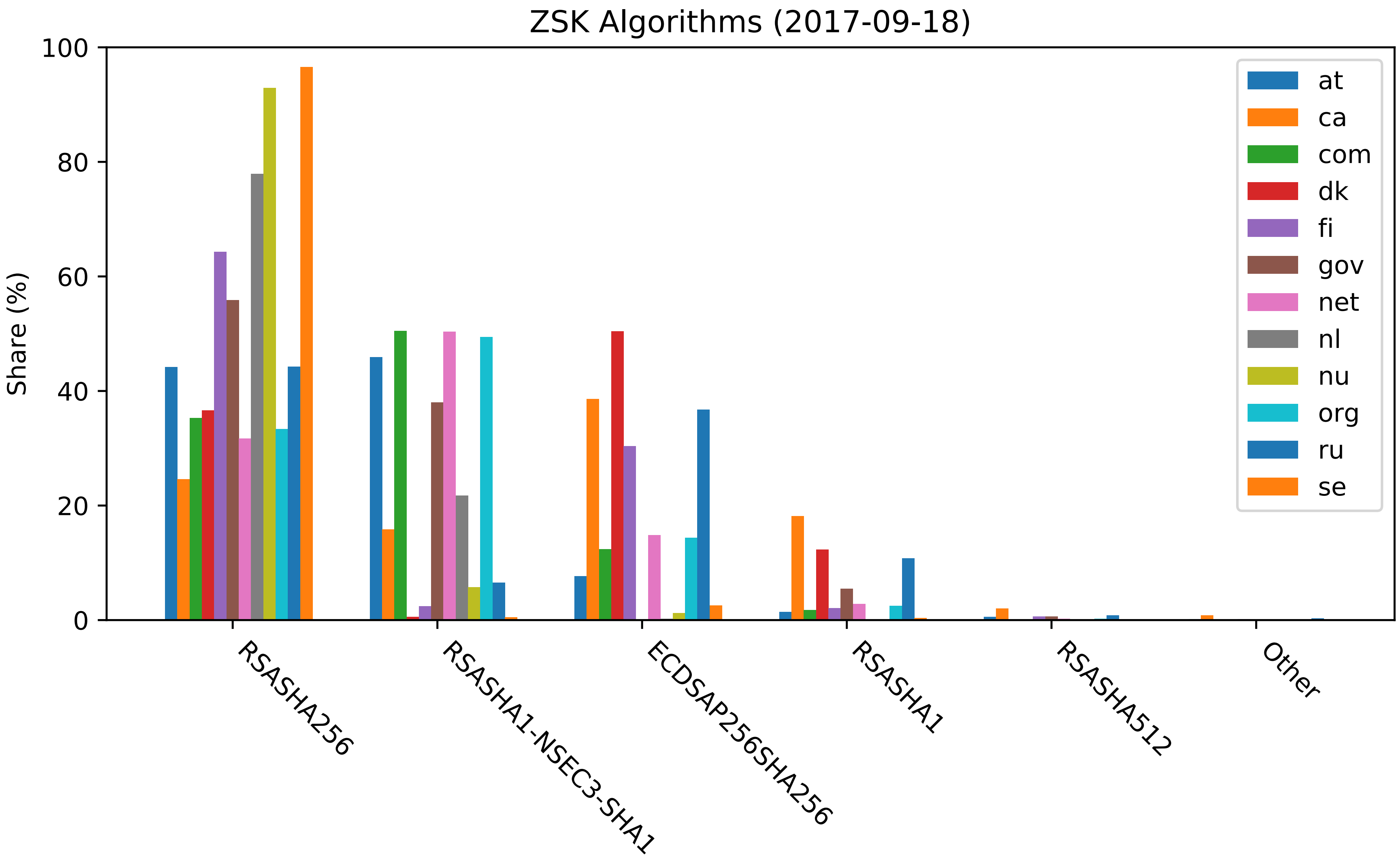
All probes (24h)



All probes (7 days)

total probe population state (24h and 7 days)

# Comparison with Signatures in the Wild



- ~ 0.1 % of the measured resolvers fail on these algorithms
- Only 13 (!) domains with RSAMD5

# Fingerprinting Resolvers

- Resolvers don’t support the same set of algorithms
  - Can we “fingerprint” resolvers based on algorithm support?
- 4,763 VPs don’t validate any algorithm

# Fingerprinting Resolvers

- 1319 VPs
- Google Public DNS

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | ❌ | 🔓 | 🔒 | 🔓 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |
| | GOST | ❌ | 🔓 | 🔒 | 🔓 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |
| | SHA-384 | ❌ | 🔓 | 🔒 | 🔓 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 398 VPs
- RFC 6725 Support

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔓 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |
| | GOST | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | SHA-384 | 🔓 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 702 VPs
- < BIND-9.9.0 (added GOST support)?

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |
| | GOST | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | SHA-384 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔒 | 🔒 | 🔓 | 🔓 |

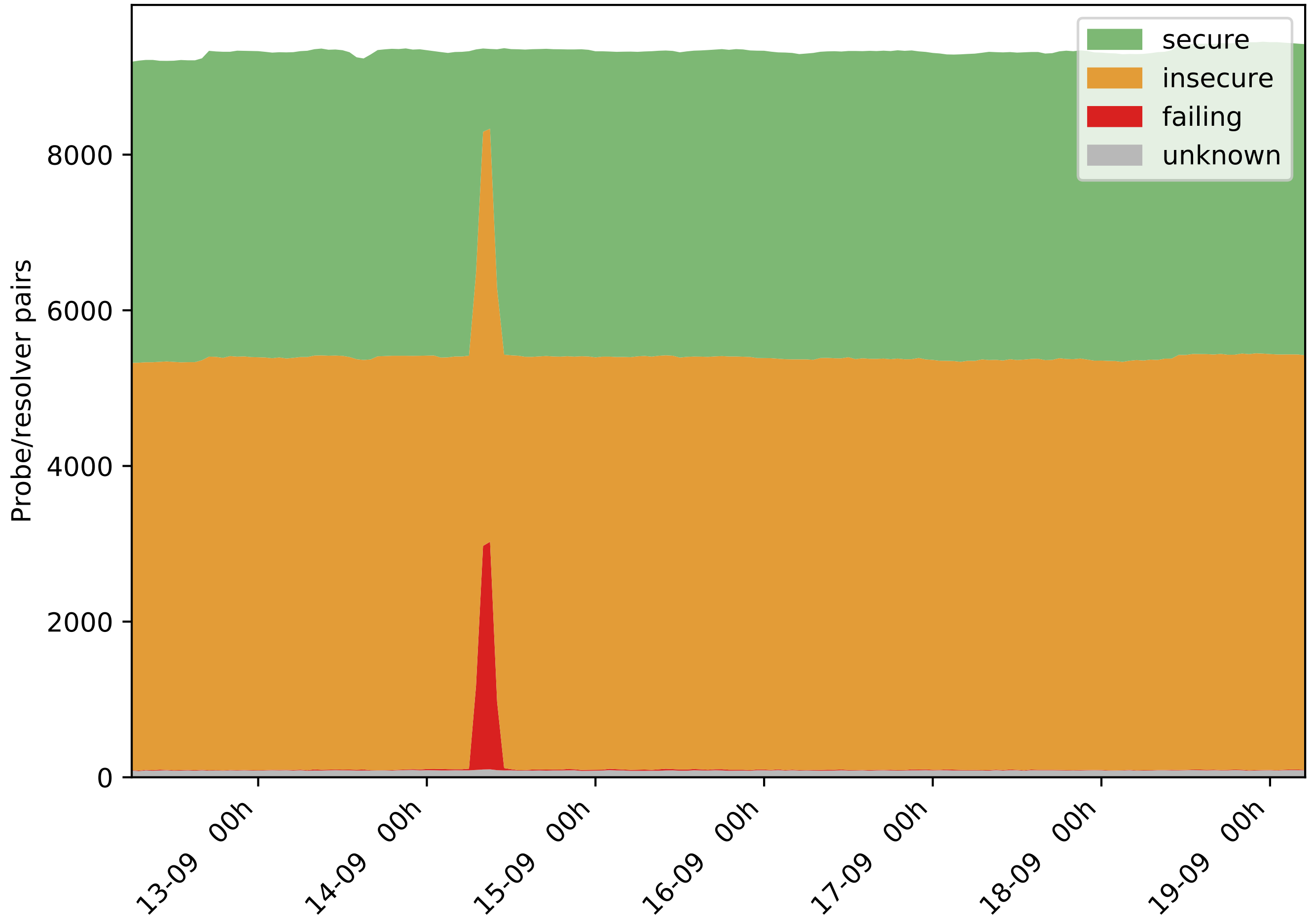
# Fingerprinting Resolvers

- 19 VPs
- PowerDNS Recursor or Knot Resolver

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | ❌ | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | ❌ | 🔓 | 🔓 | ❌ | ❌ |
| | GOST | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ | ❌ |
| | SHA-384 | ❌ | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | ❌ | 🔓 | 🔓 | ❌ | ❌ |

# Serving Stale Data?

- We’ve messed up automatic resigning

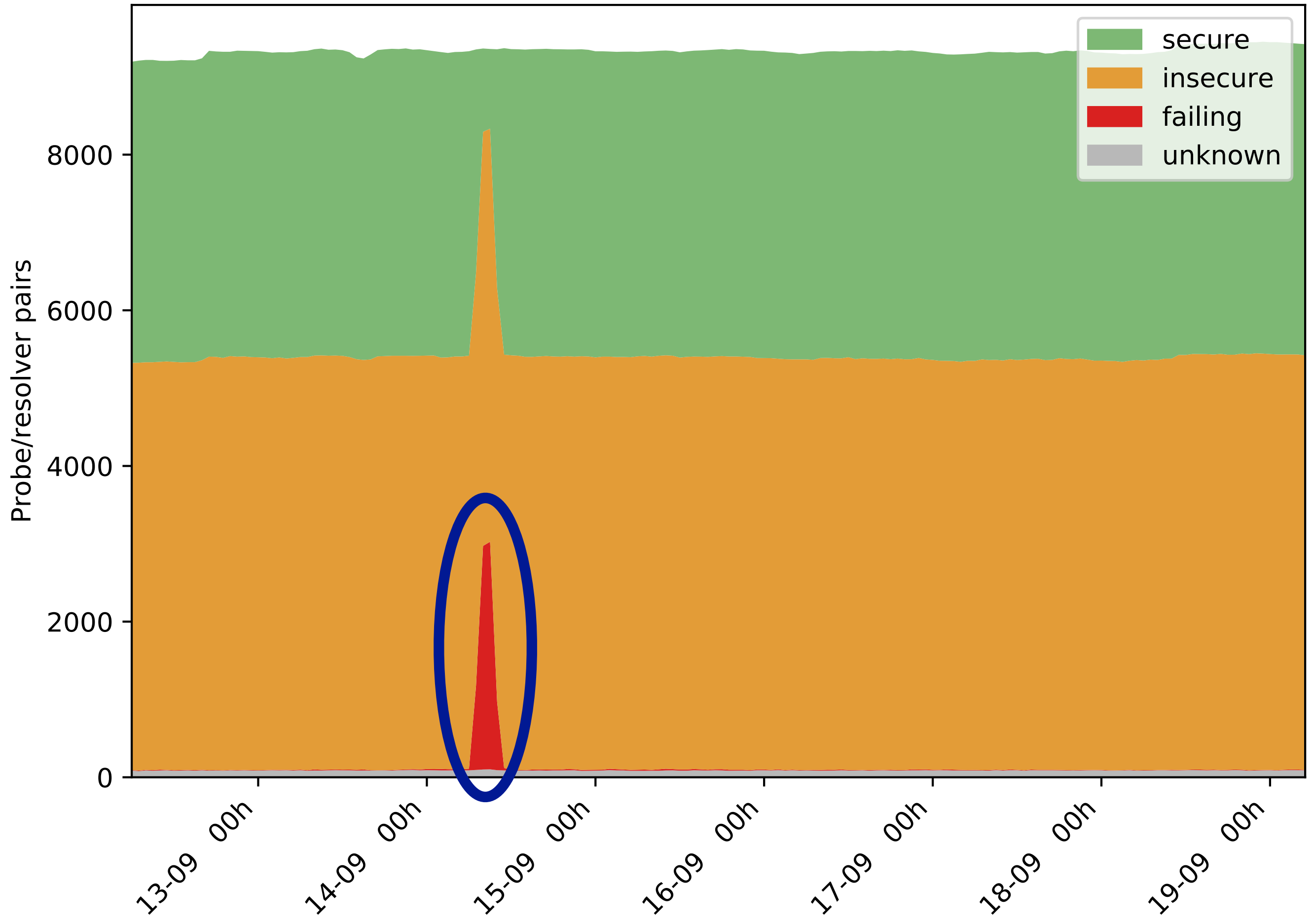


RIPE NCC
RIPE Atlas

https://rootcanary.org/

# Serving Stale Data?

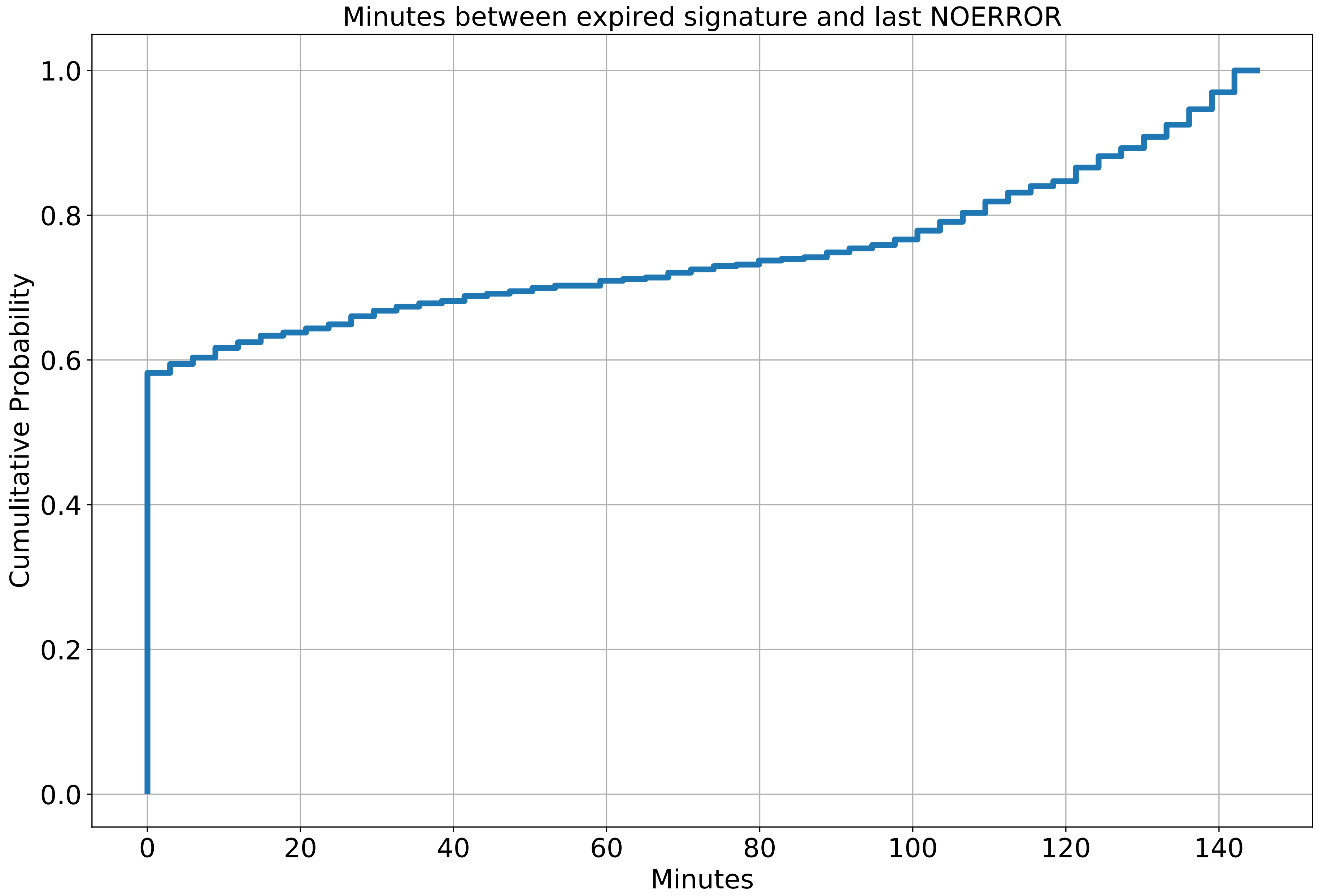
- We’ve messed up automatic resigning



RIPE NCC
RIPE Atlas

https://rootcanary.org/

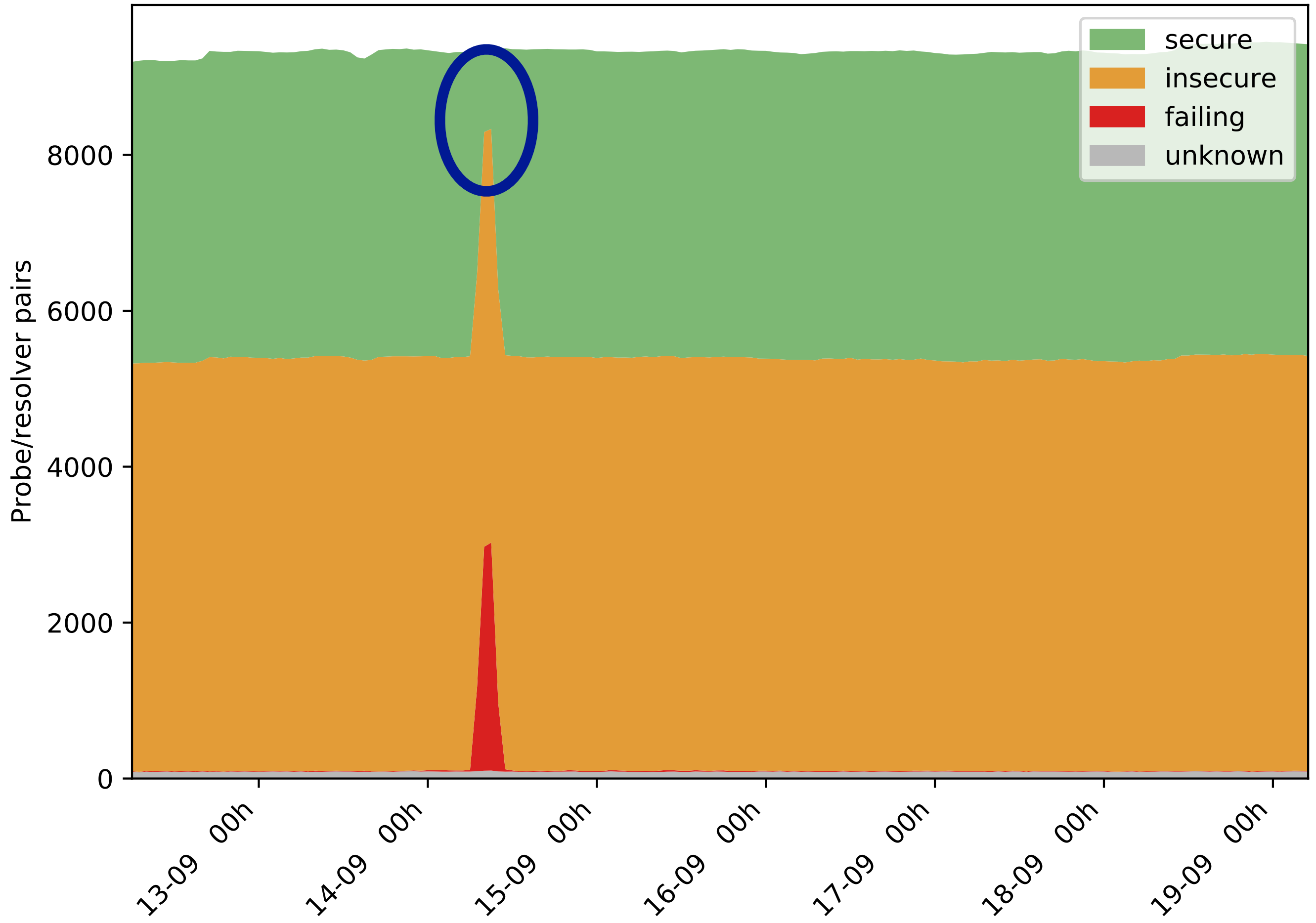
# Serving Stale Data?



https://rootcanary.org/

# Serving Stale Data?

- We’ve messed up automatic resigning



RIPE NCC
RIPE Atlas

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?

# Improving our Measurements

- Would **YOU** be willing to help us improving our measurements?

- Proposal:

  - Run small shell scripts that uses *dig* to query our test domains from within your network

  - Using the default resolvers

  - As often as possible (but at least every hour)

- Please come talk to me if you're interested

# More info

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

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

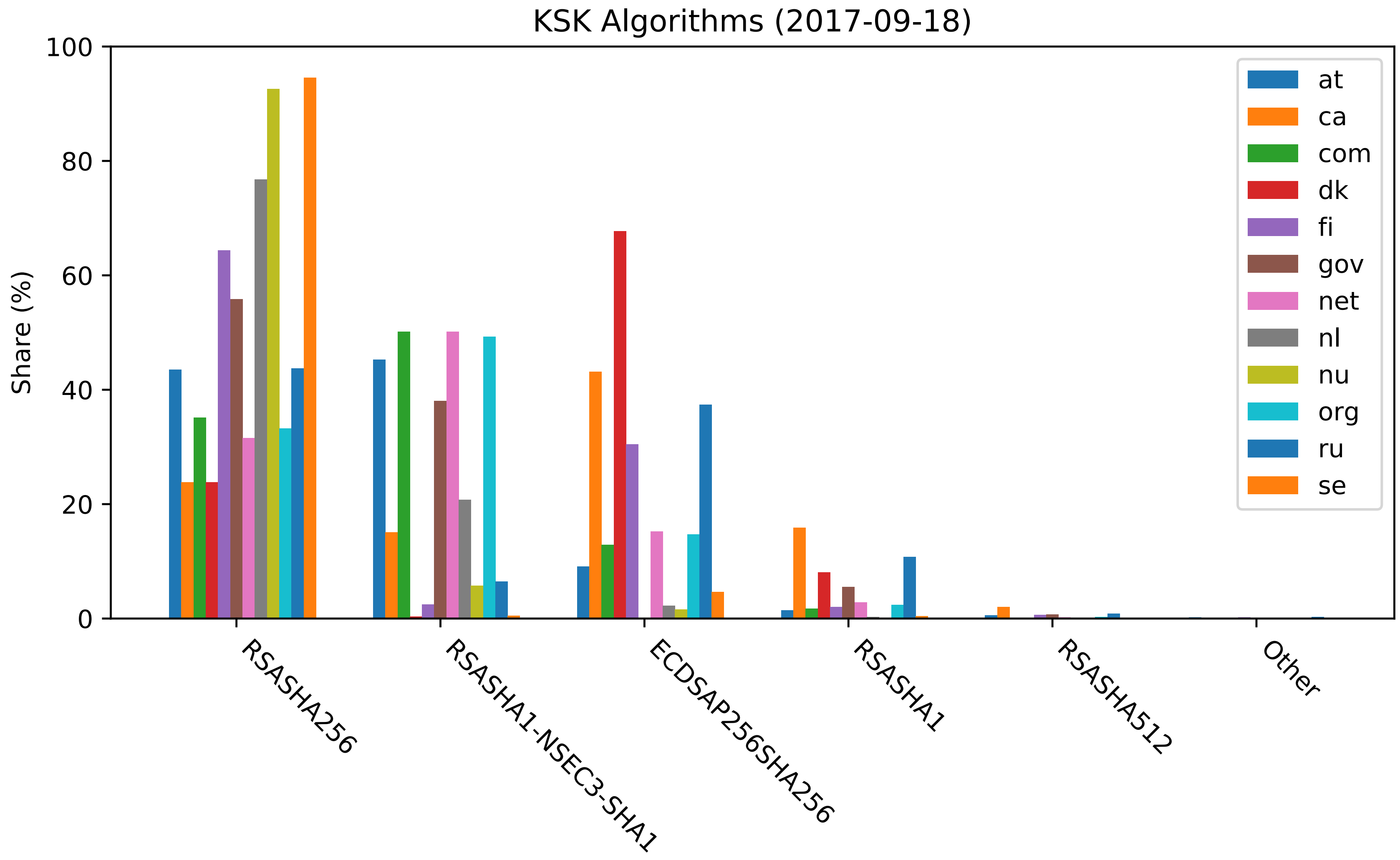
- Current results for RIPE Atlas-based measurement:
  **https://portal.rootcanary.org/rcmstats.html**

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

# The Root Canary

Bonus Slides

# Comparison with Signatures in the Wild



- 21 domains with ECC-GOST -> 12 in ru
- 1 domain with ED25519 in org

https://rootcanary.org/

# Fingerprinting Resolvers

- 394 VPs
- < BIND 9.12.0a1 (added ED448 support)?
- < PowerDNS Recursor 4.0.6 (added ED448 support)?

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 |
| | GOST | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 |
| | SHA-384 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 350 VPs
- >= Unbound 1.4.19?

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔓 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 |
| | GOST | 🔓 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 |
| | SHA-384 | 🔓 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 111 VPs
- < Unbound 1.4.7 (GOST enabled by default + no ECDSA support)?

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | GOST | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | SHA-384 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 41 VPs
- Very old Open SSL?

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔓 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | GOST | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | SHA-384 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 27 VPs

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 | 🔓 | 🔓 |
| | GOST | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 | 🔓 | 🔓 |
| | SHA-384 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |

# Fingerprinting Resolvers

- 14 VPs
- < Unbound 1.4.7

| | | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DS Algorithms | SHA-256 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | GOST | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |
| | SHA-384 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔒 | 🔓 | 🔓 | 🔓 | 🔓 | 🔓 |