Effects of KSK Roll over

Oops, so what now?

Jaap Akkerhuis
just a messenger
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
ICANN-60 NS servers

DS Algorithm

RSA-MD5
DSA
RSA-SHA1
RSA-NSEC3-SHA1
RSA-SHA1-NSEC3-SHA1
RSA-SHA256
RSA-SHA512
RSA-SHA256
EC-GOST
ECDSA-P256-SHA256
ECDSA-P384-SHA384
ED25519
ED448

DNSSEC validation succeeded for this DS and signing algorithm combination

This DS and signing algorithm combination are not validated by your resolver(s)

This DS and signing algorithm lead to a SERVFAIL

Re-run test
Google

DNSSEC validation succeeded for this DS and signing algorithm combination

This DS and signing algorithm combination are not validated by your resolver(s)

This DS and signing algorithm lead to a SERVFAIL

Re-run test
Continue measurements

Live Root Canary Monitor

Log:

Thu, 26 Oct 2017 14:11:03 GMT; ID 2876 Resolver 75.75.76.76 New State expired Old State undefined; { "nsashf_nsec_ds_sha256": []}
Root Canary was born

The Root Canary
Quantifying the Quality of DNSSEC Validation in the Wild
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

https://rootcanary.org/
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

https://rootcanary.org/
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)

https://rootcanary.org/
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

[Link: https://rootcanary.org/]
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

TCP and UDP Replies at B-Root (MIA)

TCP/UDP Ratio

TCP Replies

UDP Replies

New ZSK in Zone

https://rootcanary.org/
Canary in the virtual coalmine

- Preliminary Findings after 2017-09-19: Root

https://rootcanary.org/
Algorithm Support

- For common signing algorithms:

```
<table>
<thead>
<tr>
<th>DS Algorithm</th>
<th>SHA-256</th>
<th>SHA-384</th>
<th>GOST</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-SHA1</td>
<td><img src="green" alt="SHA-256" /></td>
<td><img src="orange" alt="SHA-384" /></td>
<td><img src="orange" alt="GOST" /></td>
</tr>
<tr>
<td>RSA-SHA1-NSEC3-SHA1</td>
<td><img src="green" alt="SHA-256" /></td>
<td><img src="orange" alt="SHA-384" /></td>
<td><img src="orange" alt="GOST" /></td>
</tr>
<tr>
<td>RSA-SHA256</td>
<td><img src="green" alt="SHA-256" /></td>
<td><img src="orange" alt="SHA-384" /></td>
<td><img src="orange" alt="GOST" /></td>
</tr>
<tr>
<td>RSA-SHA512</td>
<td><img src="green" alt="SHA-256" /></td>
<td><img src="orange" alt="SHA-384" /></td>
<td><img src="orange" alt="GOST" /></td>
</tr>
<tr>
<td>ECDSA-P256-SHA256</td>
<td><img src="green" alt="SHA-256" /></td>
<td><img src="orange" alt="SHA-384" /></td>
<td><img src="orange" alt="GOST" /></td>
</tr>
<tr>
<td>ECDSA-P384-SHA384</td>
<td><img src="green" alt="SHA-256" /></td>
<td><img src="orange" alt="SHA-384" /></td>
<td><img src="orange" alt="GOST" /></td>
</tr>
</tbody>
</table>
```

Legend:
- **green**: secure
- **orange**: insecure
- **red**: failing
- **gray**: unknown

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

https://rootcanary.org/
Algorithm Support

- Luminati vs RIPE Atlas: SHA256-RSA-SHA1

- ~ 13,000 VPs
  - 7% validating

- ~ 9,000 VPs
  - 42% validating

https://rootcanary.org/
### Fingerprinting Resolvers

- 1319 VPs
- Google Public DNS

<table>
<thead>
<tr>
<th>DS Algorithms</th>
<th>RSA-MD5</th>
<th>DSA</th>
<th>RSA-SHA1</th>
<th>DSA-NSEC3-SHA1</th>
<th>RSA-SHA1-NSEC3-SHA1</th>
<th>RSA-SHA256</th>
<th>RSA-SHA512</th>
<th>ECC-GOST</th>
<th>ECDSA-P256-SHA256</th>
<th>ECDSA-P384-SHA384</th>
<th>ED25519</th>
<th>ED448</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-256</td>
<td>🔴</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOST</td>
<td>🔴</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-384</td>
<td>🔴</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[https://rootcanary.org/](https://rootcanary.org/)
### Fingerprinting Resolvers

- 19 VPs
- PowerDNS Recursor or Knot Resolver

<table>
<thead>
<tr>
<th>DS Algorithms</th>
<th>RSA-MD5</th>
<th>DSA</th>
<th>RSA-SHA1</th>
<th>DSA-NSEC3-SHA1</th>
<th>RSA-SHA1-NSEC3-SHA1</th>
<th>RSA-SHA256</th>
<th>RSA-SHA512</th>
<th>ECC-GOST</th>
<th>ECDSA-P256-SHA256</th>
<th>ECDSA-P384-SHA384</th>
<th>ED25519</th>
<th>ED448</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SHA-256</strong></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
</tr>
<tr>
<td><strong>GOST</strong></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
</tr>
<tr>
<td><strong>SHA-384</strong></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
<td><img src="green" alt="X" /></td>
</tr>
</tbody>
</table>

[https://rootcanary.org/](https://rootcanary.org/)
Serving Stale Data?

- We’ve messed up automatic resigning

https://rootcanary.org/
Serving Stale Data?

Minutes between expired signature and last NOERROR

Cumulative Probability

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?

https://rootcanary.org/
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

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

https://rootcanary.org/
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
While waiting ...

- Twiddling thumbs
- New test might be added
Questions?