RPKI Trust Anchor Usage and Cache Consistency

John Kristoff <jtk@depaul.edu>

DePaul University (ops role)
University of Illinois at Chicago (research role)

In collaboration with:

Randy Bush <randy@psg.com>
George Michaelson <ggm@apnic.net>
Thomas C. Schmidt <t.schmidt@haw-hamburg.de>
Matthias Wählisch <m.waelisch@fu-berlin.de>
Overview of RPKI validation
Research Question

- Are RPKI cache servers consistent?
  - Why or why not?
  - How does this effect validation?
Methodology

1. Collect trust anchor repository access logs
2. Synthesize access method and server identities
3. Analyze
Synchronization Access Method

![Graph showing synchronization access method with time series data from October 2019 to June 2019. The graph compares the number of events for clients_rsync, clients_rrdp, and clients_remnant.]
RPKI Cache Server Population

24 h binning

Number of IP addresses [#]

Oct Nov Dec Jan 2019 Feb Mar Apr May Jun

afrinic_rsync
apnic_rsync
apnic_rrdp
canet_rsync
canet_rrdp
lacnic_rsync

jtk@depaul.edu
Cache Server Differences

Differences per RIR - Measured over nine cache servers

Max. Differences [%]

<table>
<thead>
<tr>
<th>Date</th>
<th>ARIN</th>
<th>RIPE</th>
<th>APNIC</th>
<th>LACNIC</th>
<th>AfriNIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>17-04-15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17-04-22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17-04-29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17-05-06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17-05-13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17-05-20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17-05-27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Auxiliary Work:
RPKI Cache and Router Discovery

- Internet Survey
  - rpki-rtr / TCP / 323
  - rpki-rtr TLS / TCP / 324
  - Routinator / TCP / 8282 (documentation example)
  - Junos / TCP / 2222 / "no problem here"
- Passive DNS survey
  - rpki*, [-.]rpki*
  - rsync traffic flows to trust anchors
Contact Info

• John Kristoff
• Email:  jtk@depaul.edu
• WWW:  https://aharp.iorc.depaul.edu
• GitHub:  https://github.com/jtkristoff
• Twitter:  https://twitter.com/jtkristoff