BGP Origin Validation (RPKI)

Authors:
Remy de Boer
<Remy.deBoer@os3.nl>
Javy de Koning
<Javy.deKoning@os3.nl>
What is RPKI?

- Designed to secure internet routing infrastructure
- Route origin validation
- Might be used for routing policies
- Certificates for proof of holdership
Why?

- BGP is currently a web of trust
- No validation or filtering can lead to outages
- Limit impact of misconfigurations
- Prevent Hijacking attempts
Research question

“How can we reliably determine which ASes are advertising invalid routes due to misconfigurations and how can we monitor this over the course of time?”
Route Origin Authorization?

- Prefix
  - (145.96.0.0/15)

- Autonomous System Number
  - (1103)

- Maximum Length (optional)
Validation states

- Unknown
  - Announcement not covered by a ROA

- Invalid
  - Announcement covered by at least one ROA but no ROA matches

- Valid
  - Announcement covered AND matched by at least one ROA
Examples (1/3)

- Advertisement:
  - Prefix: 195.169.0.0/16
  - AS number: 1103

- ROA
  - Prefix: 195.169.0.0/16
  - AS number: 1103
  - Max length: Not used ( = 16)
Examples (2/3)

- Advertisement:
  - Prefix: 181.50.0.0/22
  - AS number: 10620

- ROA
  - Prefix: 181.50.0.0/13
  - AS number: 14080
  - Max length: 24
Examples (3/3)

- Advertisement:
  - Prefix:
    - 193.48.123.0/24
  - AS number:
    - 1724

- ROA
  - Prefix:
    - 193.48.0.0/14
  - AS number:
    - 2200
  - Max length:
    - 14
RPKI Explained

BGP Updates

Validated ROA Payload

Routing Table:
- 2.2.0.2/32 from 1.0.1.1 AS: 200 I, validation-state: valid
- 172.16.1.1/32 from 1.0.1.1 AS: 200 I, validation-state: invalid
- 192.168.2.3/32 from 1.0.1.1 AS: 200 I, validation-state: unknown
Tools used

- Python/PHP/MySQL/Google Chart
- Twitter bootstrap
- RIPE RPKI Validator
- RIPE Global routing table (RIS)
- IANA address space registry
Data sources

www.ris.ripe.net/dumps

rpki.surfnet.nl

[Image of a network diagram with servers, routers, and a database, showing data flow between IPv4/6 routing table, IANA address space registry, and validated routing information.]
Measurements and Results
Global RPKI statistics

- **495838** prefixes in routing table (July 1st).
- Validation state for **14829** prefixes (2.99%).
Distribution of invalids

- Invalid AS - 730 (4.92%)
- Invalid Prefix (Fixed length mismatch) - 538 (3.63%)
- Invalid Prefix (Range length exceeded) - 480 (3.24%)
- AS & Prefix mismatch - 825 (5.56%)
- Valid - 12256 (82.65%)

Valid - 12256 (82.65%)
12256 (82.6%)
IPv4 vs IPv6

Distribution of RPKI prefixes for IPv4
- Valid - 11537 (82.21%)
- AS & Prefix mismatch - 798 (5.69%)
- Invalid Prefix (Range length exceeded) - 478 (3.41%)
- Invalid Prefix (Fixed length mismatch) - 516 (3.68%)
- Invalid AS - 705 (5.02%)

Distribution of RPKI prefixes for IPv6
- Valid - 719 (90.44%)
- AS & Prefix mismatch - 27 (3.4%)
- Invalid Prefix (Range length exceeded) - 2 (0.25%)
- Invalid Prefix (Fixed length mismatch) - 22 (2.77%)
- Invalid AS - 25 (3.14%)
Origin of invalids
## RIR Statistics

<table>
<thead>
<tr>
<th>RIR</th>
<th>Total</th>
<th>Valid</th>
<th>Invalid</th>
<th>Unknown</th>
<th>RPKI Adoption Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFRINIC</td>
<td>10839 (100%)</td>
<td>12 (0.11%)</td>
<td>0 (0%)</td>
<td>10827 (99.89%)</td>
<td>0.11%</td>
</tr>
<tr>
<td>APNIC</td>
<td>116379 (100%)</td>
<td>84 (0.07%)</td>
<td>212 (0.18%)</td>
<td>116083 (99.75%)</td>
<td>0.25%</td>
</tr>
<tr>
<td>ARIN</td>
<td>182009 (100%)</td>
<td>199 (0.11%)</td>
<td>30 (0.02%)</td>
<td>181780 (99.87%)</td>
<td>0.13%</td>
</tr>
<tr>
<td>LACNIC</td>
<td>56294 (100%)</td>
<td>5561 (9.88%)</td>
<td>1184 (2.1%)</td>
<td>49549 (88.02%)</td>
<td>11.98%</td>
</tr>
<tr>
<td>RIPE</td>
<td>128726 (100%)</td>
<td>6400 (4.97%)</td>
<td>1147 (0.89%)</td>
<td>121179 (94.14%)</td>
<td>5.86%</td>
</tr>
</tbody>
</table>
Monitoring over time

Causes of invalids

- Invalid ASN
- Invalid Prefix (Fixed length mismatch)
- Invalid Prefix (Range length exceeded)
- Invalid ASN & Prefix

Graph showing the trends over time from 18-06-13 to 01-07-13.
## Weird stuff

<table>
<thead>
<tr>
<th>Date</th>
<th>ASN</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-07-2013</td>
<td>2065</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>1942</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>1724</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>35104</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>2457</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>1937</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>1945</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>1723</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>197890</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>8649</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>ASN</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>30-06-2013</td>
<td>35104</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>8649</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>197890</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>2199</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>2471</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>27947</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>24954</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>27817</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>197860</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>9180</td>
<td>7</td>
</tr>
</tbody>
</table>
Conclusion

- Dashboard for operators and RIRs
- Distribution of invalids

Insight in:
- Configuration mistakes
- Adoption rate RPKI
- Detailed prefix information

- Daily stats monitoring
Future work

- Performance improvements
- Even more statistics
- Data already available
- Extensible framework
Q&A

- https://github.com/remydb/RPKI-Dashboard