Core Internet Functions: Routing & DNS

- The Internet relies on two critical resources
  - DNS: Translates domain names to IP addresses and IP addresses to domain names
  - Routing: Tells us how to get to an IP address
- These critical resources are not secure
- DNSSEC and RPKI secure these critical resources
What is RPKI?

• **Resource Public Key Infrastructure**
• Cryptographically certifies network resources
  – AS Numbers
  – IP Addresses
• Also certifies route announcements
  – Route Origin Authorizations (ROAs) allow you to authorize your block to be routed
Why is RPKI Important?

• Allows routers (or other processes) to validate routes
• Provides stronger validation than existing technologies, such as:
  – IRR registries
  – LOAs
  – or just “Seems legit”
Case Study: YouTube

- Pakistan Telecom was ordered to block YouTube
  - Naturally, they originated their own route for YouTube’s IP address block
- YouTube’s traffic was temporarily diverted to Pakistan
- This incident could have been prevented with widespread adoption of RPKI
Case Study: Turk Telekom

- Turkish President ordered censorship of Twitter
- Turk Telekom’s DNS servers were configured to return false IP addresses
  - So people started using Google’s DNS (8.8.8.8)
- Turk Telekom hijacked Google’s IP addresses in BGP
  - Could have been prevented with RPKI
RPKI Basics

- All of ARIN’s RPKI data is publicly available in a repository
- RFC 3779 certificates show who has each resource
- ROAs show which AS numbers are authorized to announce blocks
- CRLs show revoked records
- Manifests list all data from each organization
Hierarchy of Resource Certificates

ICANN
0.0.0.0/0
0::/0

ARIN
128.0.0.0/8
192.0.0.0/8

LACNIC

AFRINIC

RIPE

NCC

APNIC

Regional ISP
128.177.0.0/16

Other Small ISP
192.78.12.0/24

Some Small ISP
128.177.46.0/20
Route Origin Authorizations

ICANN
0.0.0.0/0
0::/0

ARIN
128.0.0.0/8
192.0.0.0/8

Regional ISP
128.177.0.0/16

Some Small ISP
128.177.46.0/20
128.177.0.0/16
AS17025

128.177.46.0/20
AS53659

Other Small ISP
192.78.12.0/24
192.78.12.0/24
AS2000

LACNIC

AFRINIC

RIPE

NCC

APNIC
Current Practices

- ARIN
  - 128.0.0.0/8
  - 192.0.0.0/8
- LACNIC
- AFRINIC
- RIPE
- NCC
- APNIC
- Regional ISP
  - 128.177.0.0/16
- Other Small ISP
  - 192.78.12.0/24
- Some Small ISP
  - 128.177.46.0/20
- Other Small ISP
  - 192.78.12.0/24
  - AS2000
Using ARIN’s RPKI Repository (Theory)

1. Pull down these files using a manifest-validating mechanism
2. Validate the ROAs contained in the repository
3. Communicate with the router to mark routes:
   - Valid
   - Invalid
   - unknown

Ultimately, the ISP uses local policy on how to route to use this information.
Using ARIN’s RPKI Repository (Practice)

1. Get the RIPE NCC RPKI Validator

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Trust anchor</th>
<th>Processed Items</th>
<th>Expires in</th>
<th>Last updated</th>
<th>Next update in</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>APNIC from AFRINIC RPKI Root</td>
<td>13 1 0</td>
<td>2 years and 11 months</td>
<td>15 minutes ago</td>
<td>Updating ROAs</td>
</tr>
<tr>
<td></td>
<td>APNIC from ARIN RPKI Root</td>
<td>130 1 0</td>
<td>4 years and 8 months</td>
<td>15 minutes ago</td>
<td>Updating ROAs</td>
</tr>
<tr>
<td></td>
<td>APNIC from IANA RPKI Root</td>
<td>2530 1 0</td>
<td>4 years and 8 months</td>
<td>14 minutes ago</td>
<td>Updating ROAs</td>
</tr>
<tr>
<td></td>
<td>APNIC from LACNIC RPKI Root</td>
<td>6 0 0</td>
<td>2 years and 11 months</td>
<td>4 seconds ago</td>
<td>10 minutes</td>
</tr>
<tr>
<td></td>
<td>APNIC from RIPE RPKI Root</td>
<td>28 1 0</td>
<td>4 years and 8 months</td>
<td>15 minutes ago</td>
<td>Updating ROAs</td>
</tr>
<tr>
<td></td>
<td>ARIN RPKI Root</td>
<td>1916 3 0</td>
<td>9 years and 7 months</td>
<td>8 minutes ago</td>
<td>2 minutes</td>
</tr>
<tr>
<td></td>
<td>AfriNIC RPKI Root</td>
<td>387 0 0</td>
<td>9 years and 11 months</td>
<td>9 minutes ago</td>
<td>1 minute</td>
</tr>
<tr>
<td></td>
<td>LACNIC RPKI Root</td>
<td>3448 0 1</td>
<td>5 years and 2 months</td>
<td>5 minutes ago</td>
<td>5 minutes</td>
</tr>
<tr>
<td></td>
<td>RIPE NCC RPKI Root</td>
<td>17182 0 0</td>
<td>4 years and 10 months</td>
<td>13 minutes ago</td>
<td>Updating ROAs</td>
</tr>
</tbody>
</table>
Using ARIN’s RPKI Repository (Practice, continued)

2. Get the ARIN TAL
   – https://www.arin.net/resources/rpki/tal.html

3. Plug it in to your routing policy engine:
   – Directly to the router via RTR protocol
   – Using custom scripts and the REST API
   – As RPSL route objects
Putting Your Routes in the RPKI

1. Determine if you want to allow ARIN to host your Certificate Authority (CA), or if you want ARIN to delegate to your Certificate Authority.
2. Sign up with ARIN Online.
3. Create Resource Certificates and ROAs.
Hosted vs. Delegated RPKI

• Hosted
  – ARIN has done all of the heavy lifting for you
  – Think “point click ship”
  – Available via web site or RESTful interface

• Delegated using Up/Down Protocol
  – A whole lot more work
  – Might make sense for very large networks
Hosted RPKI - ARIN Online

• **Pros**
  – Easy-to-use web interface
  – ARIN-managed (buying/deploying HSMs, etc. is expensive and time consuming)

• **Cons**
  – Downstream customers can’t use RPKI
  – Large networks would probably need to use the RESTful interface to avoid tedious management
  – We hold your private key
Delegated RPKI with Up/Down

• **Pros**
  – Allows you to keep your private key
  – Follows the IETF up/down protocol
  – Allows downstream customers to use RPKI

• **Cons**
  – Extremely hard to set up
  – Requires operating your own RPKI environment
  – High cost of time and effort
Delegated with Up/Down

• You have to do all the ROA creation
• Need to set up a Certificate Authority
• Have a highly available repository
• Create a CPS
# RPKI Usage

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Orgs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>47</td>
<td>68</td>
<td>108</td>
<td>153</td>
<td>187</td>
<td>220</td>
<td>250</td>
<td>268</td>
<td>292</td>
<td></td>
</tr>
<tr>
<td>ROAs</td>
<td>19</td>
<td>60</td>
<td>106</td>
<td>162</td>
<td>239</td>
<td>308</td>
<td>338</td>
<td>370</td>
<td>414</td>
<td>470</td>
</tr>
<tr>
<td>Covered Resources</td>
<td>30</td>
<td>82</td>
<td>147</td>
<td>258</td>
<td>332</td>
<td>430</td>
<td>482</td>
<td>528</td>
<td>577</td>
<td>640</td>
</tr>
<tr>
<td>Up/Down Delegated</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
RPKI vs The Routing Table: Globally

Global: Validation Snapshot of Unique P/O pairs
730,286 Unique IPv4 Prefix/Origin Pairs

- not-found (668,659) 91.56%
- valid (55,539) 7.61%
- invalid (6,088) 0.83%

NIST RPKI Monitor 2017–09–10
RPKI vs The Routing Table: RIPE

RIPE: Validation Snapshot of Unique P/O pairs
181,812 Unique IPv4 Prefix/Origin Pairs

- not-found (153,739)
- valid (25,957)
- invalid (2,116)

invalid 1.16%
valid 14.28%
not-found 84.56%

NIST RPKI Monitor 2017-09-10
RPKI vs The Routing Table: APNIC

APNIC: Validation Snapshot of Unique P/O pairs
192,250 Unique IPv4 Prefix/Origin Pairs

- not-found (182,843)
- valid (7,586)
- invalid (1,821)

invalid 0.95%
valid 3.95%
not-found 95.11%

NIST RPKI Monitor 2017-09-10
RPKI vs The Routing Table: AFRINIC

AfriNIC: Validation Snapshot of Unique P/O pairs
19,018 Unique IPv4 Prefix/Origin Pairs

- not-found: 18,735 (98.51%)
- valid: 261 (1.37%)
- invalid: 22 (0.12%)

NIST RPKI Monitor 2017-09-10
RPKI vs The Routing Table: LACNIC

LACNIC: Validation Snapshot of Unique P/O pairs
78,276 Unique IPv4 Prefix/Origin Pairs

- not-found (58,522) - valid (18,294) - invalid (1,460)

- invalid 1.87%
- valid 23.37%
- not-found 74.76%

NIST RPKI Monitor 2017-09-10
RPKI vs The Routing Table: ARIN

ARIN: Validation Snapshot of Unique P/O pairs
258,908 Unique IPv4 Prefix/Origin Pairs

- not-found (254,798) - valid (3,441) - invalid (669)

- invalid 0.26%
- valid 1.33%
- not-found 98.41%

NIST RPKI Monitor 2017-09-10
Takeaways

• If you’re not using RPKI, you’re vulnerable to route hijacking
• Plenty of readily available documentation regarding implementation details
• If we can help, contact us
RPKI vs IRR

- RPKI could provide closer to real-time route validation
- IRR is mostly used to generate filters
- Maybe use RPKI within IRR for better validation of data
  - https://www.nanog.org/meetings/nanog43/presentations/DanMcP_Route_Filter_Panel_N43.pdf
- Many have strong opinions for/against each approach
IRR

• Been around for decades
  – RIPE-181 published in 1994
  – Varying degree of success

• ARIN’s IRR
  – Uses old IRR software from RIPE that is bolted to the side
  – Really showing its age, not customer friendly
IRR within the ARIN Region

- There are five suggestions (ACSPs in ARIN-lingo) to improve the IRR
  - Two where completed over the years
- Community Consultation was in favor of upgrading the IRR
IRR Themes

- Improve the validity of the IRR data
- Work with the other RIR’s on authorization schemes
- Provide appropriate proxy registration services
- Integrate/validate with the registration database
- Cross reference RPKI work where appropriate
How this is to be done

• Work with the community to produce a Simplified Profile of RPSL
  – Use RESTful services
  – Make it simple
• Collaborate with the other RIR’s on cross-authentication
• Provide an easy way to integrate IRR functions within ARIN Online
Q&A