NLNET LABS?
Purveyors of fine open source software since 1899
ROUTINATOR

A NEW NLNET LABS PROJECT
RPKI TOOLS

Announcements

- Valid: 1155
- Invalid ASN: 0
- Invalid Length: 3
- Not Found: 28

Payloads

- Verified ROA Payloads: 805
- Unseen: 12

The fraction of announced IPv4 and IPv6 prefixes in BGP covered by RPKI ROAs.

nlnetlabs.nl/projects/rpki/rpki-analytics/
RPKI
It’s all about Resources.

Internet Number Resources to be precise...
The RPKI certificate structure follows the Internet resource allocation hierarchy.
PUBLISHING RPKI DATA
SEPARATE COMPONENTS

CERTIFICATE AUTHORITY

creates & signs

PUBLICATION SERVER

makes available
“Is this BGP origination authorised by the legitimate holder of the address space?”
ROUTE ORIGIN AUTHORISATION

- AS Number
- IP Prefix
- Maximum Prefix Length (maxLength)

Liberal usage of maxLength opens up the network to a forged origin attack. ROAs should be as precise as possible.
ROV: THREE POSSIBLE OUTCOMES

• Valid
  ✦ The route announcement is covered by at least one Validated ROA Payload

• Invalid
  ✦ The prefix is announced from an unauthorised AS, or the announcement is more specific than is allowed by the maxLength set in a VRP that matches the prefix and AS.

• Not Found
ORIGIN VS. PATH VALIDATION

- Route Origin Validation (ROV) provides value for most issues:
  - Most mis-originations are accidental – “fat-fingering”
  - For many networks, the most important prefixes are one hop away
- Practical Path Validation is achievable, drafts are in progress:
  - draft-azimov-sidrops-aspa-profile
  - draft-azimov-sidrops-aspa-verification
HOSTED RPKI

- All five RIR have been offering Hosted RPKI since 2011
- Request certificate and issue ROAs through web portal
- Implementations vary across regions:
  - ROA Request Generation Key Pairs in ARIN
  - User interface guidance to create high quality ROAs
  - Setting up alerts for misconfigurations and possible hijacks
RIPE NCC
RIPE Network Coordination Centre

You are here: Home > Manage IPs and ASNs > LIR Portal

My LIR

Resources
- My Resources
- Request Resources
- Request Transfer
- IPv4 Transfer Listing Service
- RPKI Dashboard
- RIPE Database

RPKI Dashboard

2 BGP Announcements
- 2 Valid
- 0 Invalid
- 0 Unknown

2 ROAs
- 2 OK
- 0 Causing problems

BGP Announcements

<table>
<thead>
<tr>
<th>AS number</th>
<th>Prefix</th>
<th>Most specific length allowed</th>
<th>Affects</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS199664</td>
<td>2a04:b900::29</td>
<td>29</td>
<td>1</td>
</tr>
<tr>
<td>AS199664</td>
<td>185.49.140.0/22</td>
<td>22</td>
<td>1</td>
</tr>
</tbody>
</table>

History

Search...
DELEGATED RPKI

- Better integration with operator’s own systems
- Organization will be the only one in possession of their private key
- Organization is operationally independent from the parent RIR
- Operator of a global network can operate a single system, rather than maintain ROAs in up to five web interfaces
WHATEVER YOU CHOOSE, GO ALL IN!

• It’s better to create **no** ROAs than **bad** ones

• Once you start create ROAs, **maintain** them!

• Make RPKI part of standard operations

• Set up monitoring and alerting

• Train your first line help desk
WHAT IF IT BREAKS?

- No DNSSEC horror story; e.g. unavailable zone due to signing mishap
- RPKI provides a positive statement on routing intent
- Lose your keys? Hardware failure? Publication server being DDOSed?

All routes will eventually fall back to the “NotFound” state, as if RPKI were never used
USING RPKI DATA
RPKI VALIDATION

LACNIC repository

ARIN repository

NIR repository

LIR repository

RELYING PARTY SOFTWARE

validated cache

rsync

RPKI-RTR
For ROV to succeed in its objective, operators should ultimately drop all BGP announcements that are marked as Invalid.
FURTHER READING
RPKI DOCUMENTATION PROJECT

https://rpki.readthedocs.io