RPKI, what we've learned and what we've been doing

SANOG38/npNOG6

vivek@apnic.net

Resource Public Key Infrastructure

What is RPKI?

A robust security framework for verifying the association between **resource holders** and their **Internet number resources**.

Route Origin Authorization

What is contained in ROA?

- – The AS number you have authorized
- – The prefix that is being originated from it
- – The most specific prefix (maximum length) that the AS may announce

eg : "ISP 4 permits AS65551 to originate a route for the prefix 198.51.100.0/24"

RPKI Initiatives

Initial challenge was to get APNIC Members to create ROAs

10 face-to-face and eLearning RPKI training courses delivered

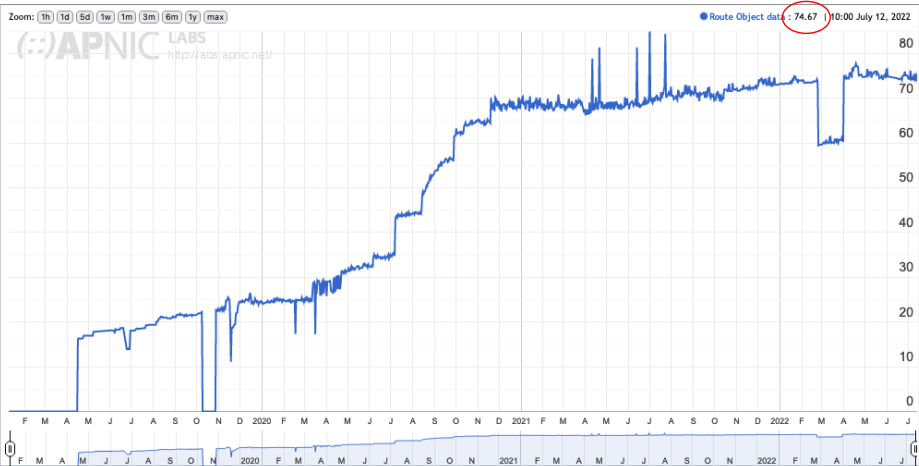RPKI presentations to NOGs and conferences

Development of the 'Ready to ROA' campaign – hands on sessions to help Members create ROAs

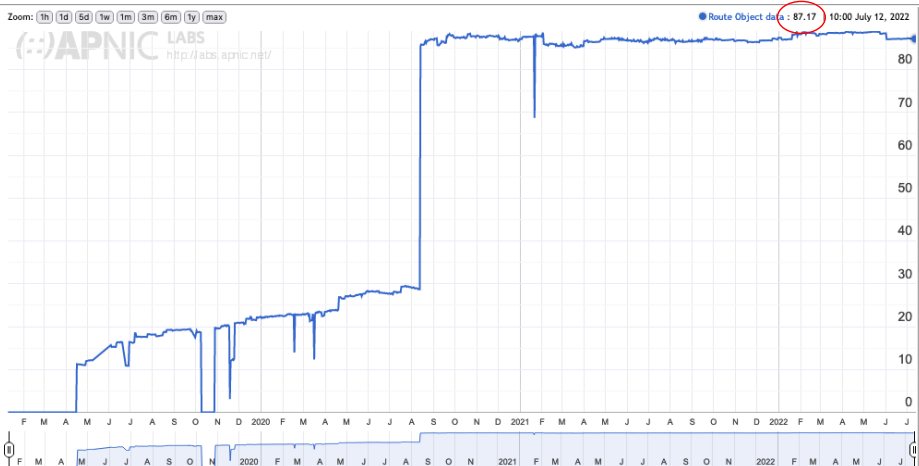New shirts, stickers, web content to promote campaign

Ready to ROA launched in 2015

ROA coverage – South Asia

https://stats.labs.apnic.net/roas

Route Origin Validation

Status

Displaying 30 major operators [+ Show all] [+ Show ASN column]

NAME	TYPE	DETAILS	STATUS ▲
Lumen	transit	signed + filtering	safe
Arelion (Formally Telia)	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
TATA	transit	signed + filtering	safe
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Comcast	ISP	signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Amazon	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
Wikimedia Foundation	cloud	signed + filtering	safe
Scaleway	cloud	signed + filtering	safe

https://isbgpsafeyet.com/

RPKI invalids

Rise of the invalids
By Tashi Phuntsho on 10 Apr 2020

RPKI invalids are not going away
By Md Abdul Awal on 16 Jul 2021

Solo effort to clean up RPKI invalids across a region
By Peter Peele on 26 Jul 2021

RPKI invalids

- On 27 April 2021, we saw 3526 RPKI invalid routes for IPv4 addresses delegated to APNIC Members

Validation result	IPv4 count	IPv6 count
Invalid AS	556	37
Invalid AS and ML	456	24
Invalid ML	2514	456
Total	**3526**	**517**

Table 1 — Validation counts for IPv4 and IPv6 on 27 April 2021, collected from Routeviews collector SG and Routinator 0.8.3.

Cleaning up RPKI invalids

Cleaning up your RPKI invalid routes
By Vivek Nigam on 28 Apr 2021

Fixing your incorrect or outdated ROAs is easy — here's how.

- Email campaign in June 2021 to reach out to Members with RPKI invalid announcements

ROA creation interface

Add new   ✕

Prefix	61.45.250.0/23
Origin AS	The AS number that is authorized, e.g. AS65536
ℹ Max length	/23
ℹ ROA	☑ Enabled (ROAs will be created for this route)
Whois	☐ Enabled (Whois route objects will be created for this route)
Options	☐ Notify additional contacts

Cancel   Next

Improved ROA creation interface

Routing status alerts in DASH

https://dash.apnic.net/

Routing status alerts in DASH

Routing status alerts in DASH

ROA mismatch for 103.21.244.0/24   ✕

Reason: The prefix length seen in BGP does not match with the ROA maxlength.

Length in **BGP**:   Scope in **ROA** ⓘ :
/24   /23 - /23 (103.21.244.0/23 - AS0)

Required actions:

- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. Learn more about BGP hijacking. ⌄

- If you did not expect this max length, review the ROAs for this prefix.

Close

Reducing ROA downtime during transfers

- Facilitate resource transfers involving live networks

- Existing ROAs published for 2 weeks after transfers

APNIC

What we've learned?

Upcoming RPKI improvements

- Routing status alerts notification

- ROA pre-validation

- Registry API
  - https://blog.apnic.net/2022/03/22/apnic-registry-api/

- New ROA guides and Help Centre articles

Thank you!