



RIPE NCC
RIPE NETWORK COORDINATION CENTER

RPKI-flutter

A high-resolution RPKI observatory

Emile Aben, Ties de Kock, Agustín Formoso | RIPE NCC | 2024-10-29

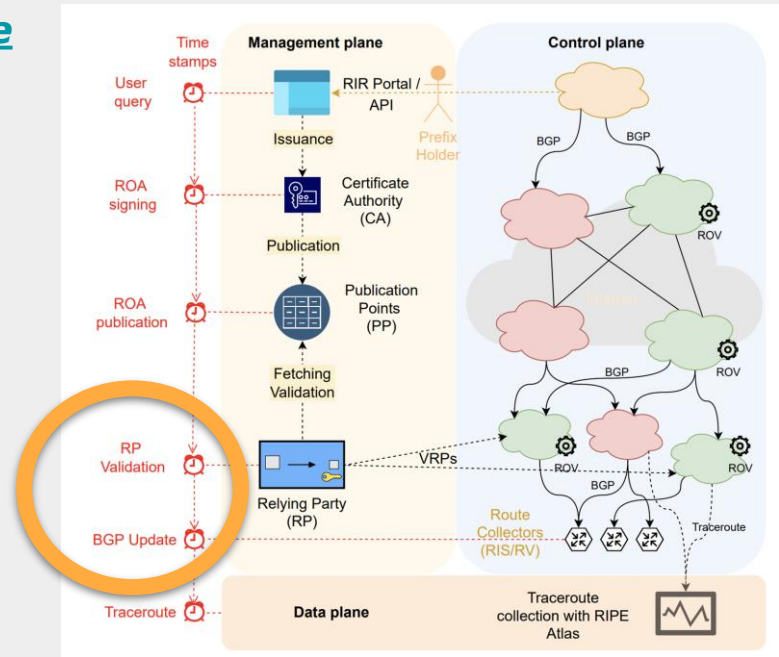
How do RPKI and BGP interact?



From [RPKI Time-of-Flight: Tracking Delays in the Management, Control, and Data Planes](#):

“We observe significant disparities in ISPs’ reaction time to new RPKI information, ranging from a few minutes to one hour”

What does this look like “in the wild” ?



Enter “RPKI-flutter”



We built a data collection prototype:

“RPKI-flutter”

Goal: Observe changes in RPKI outputs at high time granularity

By-catch: Interesting low volume RPKI dataset, potentially filling a gap in near-realtime observability and post-mortem analysis



How does RPKI-flutter collect data?



We poll 4 Routinator instances for VRP Up/Down:

- Snapshot of state at start of day ("bview")
- VRP Up/Down every 30s ("updates")

Daily [parquet](https://rd-www-1.ripe.net/rpki_flutter/daily/) aggregate at: https://rd-www-1.ripe.net/rpki_flutter/daily/

```
AS21515 137.119.26.0/23 23
AS21515 137.119.64.0/20 20
AS15353 23.145.56.0/24 24
AS60900 23.145.57.0/24 24
AS15353 170.39.49.0/24 24
AS263080 187.33.48.0/21 24
AS263080 189.201.208.0/20 24
AS263080 2804:964::/32 64
```

	Granularity	Vantage points	Daily volume	Pre validation data	Post validation data
RIPE NCC RPKI archive	daily	1	750 MB	yes	yes
RPKIviews	15 min	5	180 GB	yes	yes
RPKI-flutter	<= 30 sec	4	30 MB	no	yes

The Interface: Compare RPKI and BGP Timing



This interface allows you to select and zoom in to individual VRPs and exact BGP matches

Limitations: ie. future work :)

- Not looking at more/less specific prefixes yet
- BGP data only as recent as current BGPlay API

"RPKI-flutter" and BGP

This prototype explores the interaction of **RPKI VRPs** and **BGP** at high time granularity. We capture VRP state changes (ie. announce or withdrawal) at a handful of vantage points. To distinguish this from BGP state changes we call these "flutter" events. To explore this, first select a date below. After that you will get a list of VRPs that we see fluttering on that day. There is an optional filter available below, if you want to quickly narrow this down. For instance to your own ASN.

Date

On **2024-10-23** we captured **1318** VRPs that are fluttering. Note the plot

<https://observablehq.com/@emileaben/rpki-flutter-and-bgp>

Example Observation: Top flutterer



This Amazon VRP keeps being added/removed

View from our 4 VPs is different!

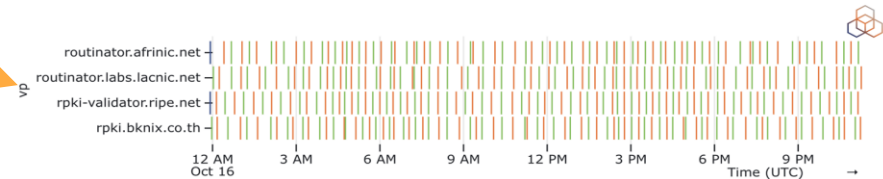
No prefix in BGP that matches this

Amazon is monitoring the RPKI [1]

AS400098 199.36.120.0/24 24 fluttered 335 times on 2024-10-16

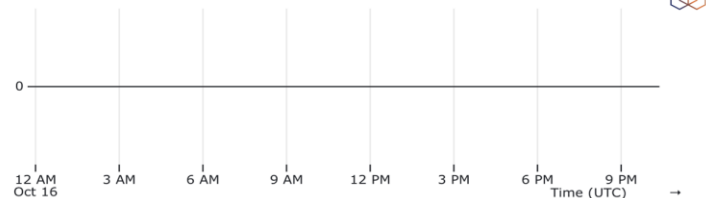
VRP visibility per vantage point

State VRP Up VRP Down



BGP Origin visibility

RIS peers seeing



[1] <https://manrs.org/2023/10/coordination-key-to-largest-rpki-deployment/>

Example Observation: BGP Churn, but no visibility change



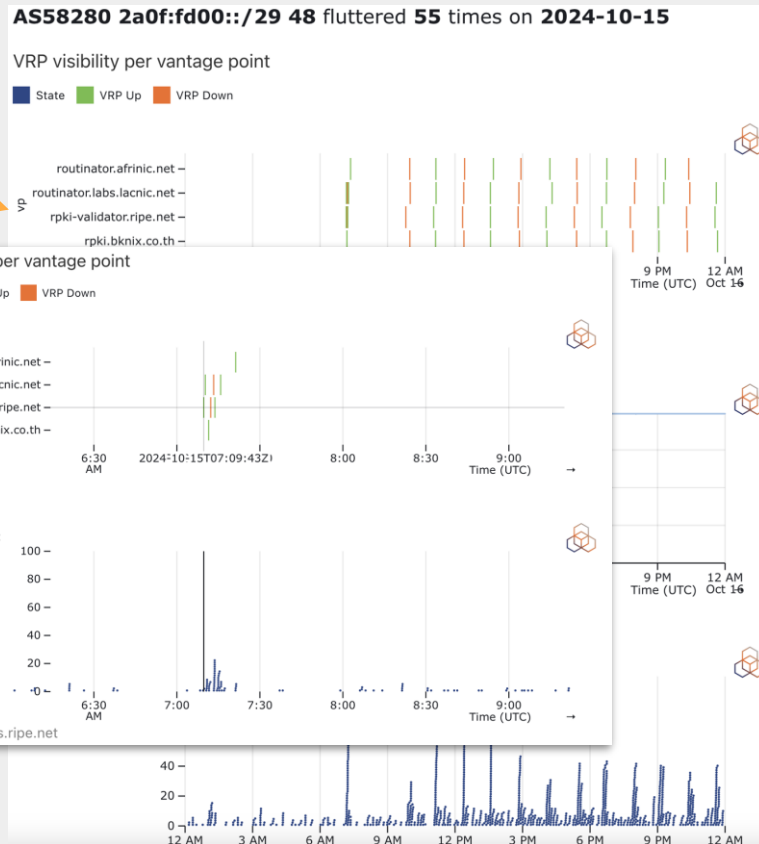
Test in collaboration with Max Stucchi (AS58280):

Changing VRP so BGP prefix RPKI status flapped between **'Valid'** and **'NotFound'**

No change in BGP visibility, prefix was not withdrawn (as expected)

But noticeable BGP update churn, see [1]

Interesting artefacts if you zoom



[1] <https://labs.ripe.net/author/stucchimax/a-bgp-side-effect-of-rpki/>

Example Observation: IP Leasing Enforcement?



A VRP appears for a prefix that is announced by another ASN. No other VRPs

=> prefix becomes "invalid"

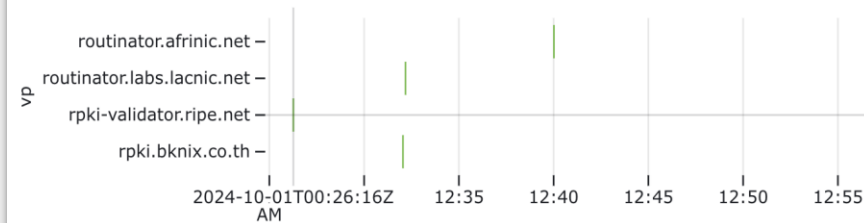
BGP visibility of the prefix drops significantly

Zoom in shows when BGP change starts and reaches maximum effect

=> BGP changes happen in the 20-30 mins after VRP change

VRP visibility per vantage point

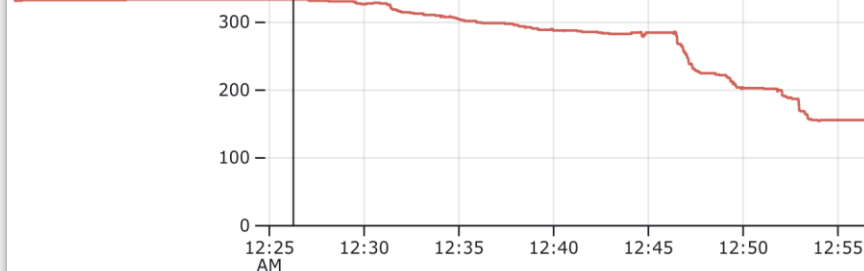
State VRP Up VRP Down



BGP Origin visibility

140.233.167.0/24 14445 140.233.167.0/24 47585

↑ RIS peers seeing



Conclusion



We make a flutter notebook available for netops (post mortem use-case) and researchers:

<https://observablehq.com/@emileaben/rpki-flutter-and-bgp>

We make the flutter data available:

https://rd-www-1.ripe.net/rpki_flutter/daily/

Wishlist:

- Make this VRP-to-BGP observatory near-real time
- Other vantage points (other validators^w relying-party software)
- If you find an interesting case, please post on social media (tag #RPKIFlutter)

Feedback appreciated!



Questions & Comments



emile.aben@ripe.net