RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Recent developments in routing security

Theodoros Polychniatis
Manager Business Applications

Theodoros Polychniatis | GRNOG14 | 3 May 2023

BGP is based on trust

- **Any** network (ASN) can announce **any** IP prefix

- No built-in security in BGP protocol

- Malicious or misconfigured sources can potentially propagate fake routing information all over the Internet

Routing security programme

- **Internet Routing Registry (IRR)**

  - Collection of databases for routing purposes

  - RIPE, APNIC, RADB, JPIRR, Level3, NTTCom, others

  - Which prefixes originate from which AS

  - Routing policies (advertised/accepted prefixes)

- **RPKI**

  - Security framework

  - Proves holdership through a public key and certificate infrastructure

  - Is the originating ASN authorised to originate a particular prefix?

Resource
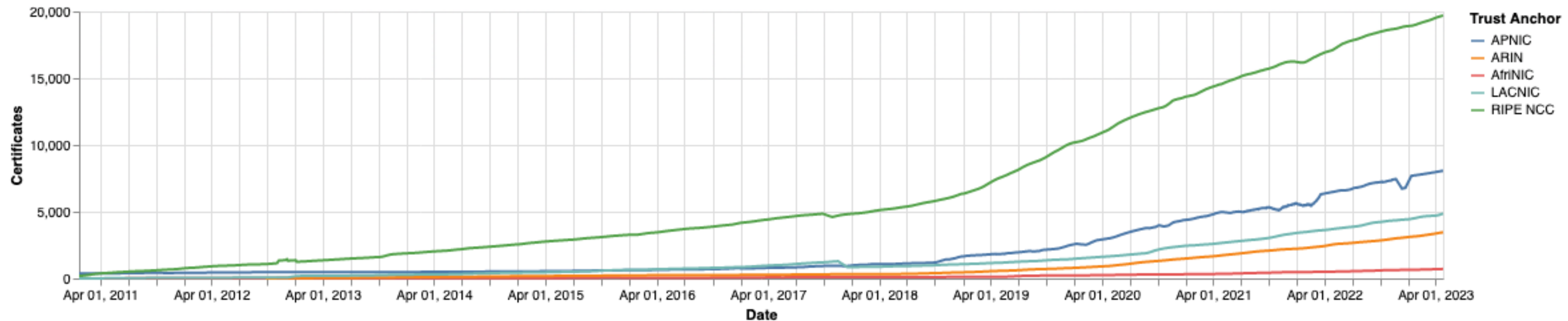**P**ublic
Key
Infrastructure

RPKI

RPKI Statistics

- Steady growth in adoption and number of ROAs

  - **93%** of the **IPv4** space and **41%** of the **IPv6** in Greece is covered by ROAs

  - https://ftp.ripe.net/pub/stats/ripencc/nro-adoption/latest

  - https://certification-stats.ripe.net/

RPKI validators are mature (1)

- Much better as compared to five years ago

- Installation, configuration, documentation is way better

- Many security vulnerabilities exposed from 2021 research have been fixed

  - https://arxiv.org/pdf/2203.00993.pdf

RPKI validators are mature (2)

- Risk of monoculture, so run different validators

  - https://rov-measurements.nlnetlabs.net/stats/

  - Routinator - 80%

  - rpki-client - 8%

  - OctoRPKI - 6%

  - Fort - 3%

  - RIPE NCC RPKI Validator 3 - 3%   **[STOP USING IT IF YOU STILL DO]**
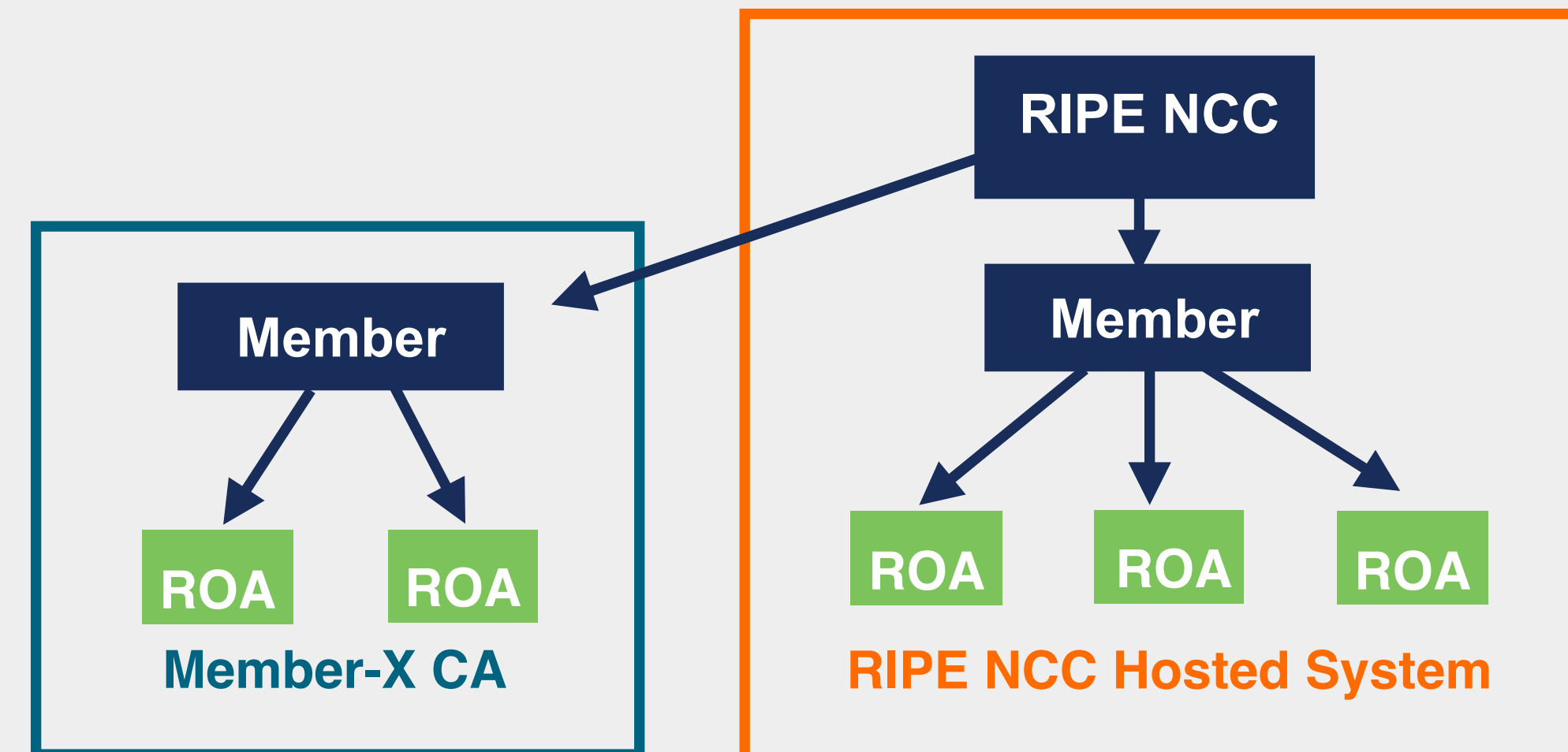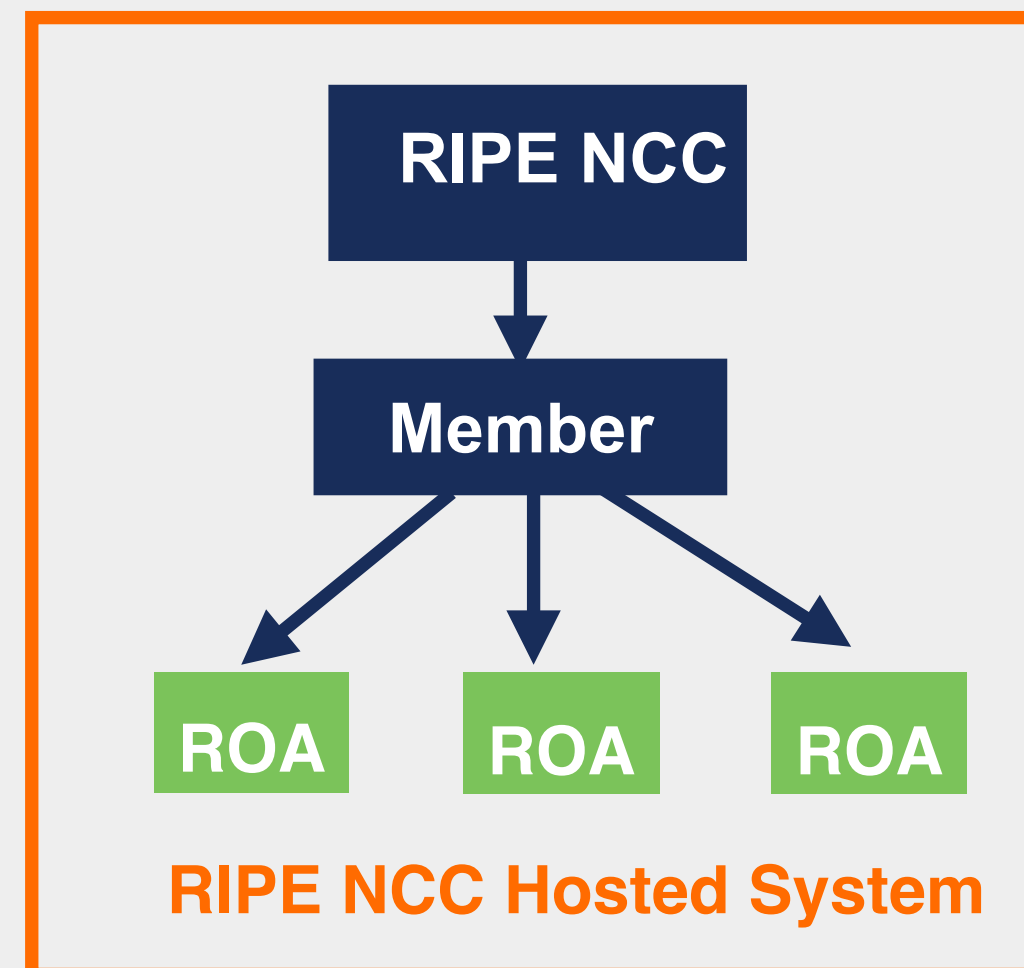
RPKI Flavours

- **Hosted RPKI**

  - RIRs host CAs for LIRs

  - Automated signing and key rollovers

 - Information published in RIR repository

- **Delegated RPKI**

  - LIR manages its own RPKI system

  - Runs its own CA, manages its own keys/ key rollovers

  - Creates ROAs in its own platform

New: Publication as a Service

- LIR manages full RPKI system

- Runs its own CA, manages its own keys/ key rollovers

- Creates ROAs in its own platform

- **LIR publishes ROAs in RIR's repository**

- RIRs have experience in maintaining consistency and better availability

- Well-documented and easy to set up

- Supported by APNIC, ARIN, RIPE NCC, NIRs

- A win-win for smaller delegated CAs
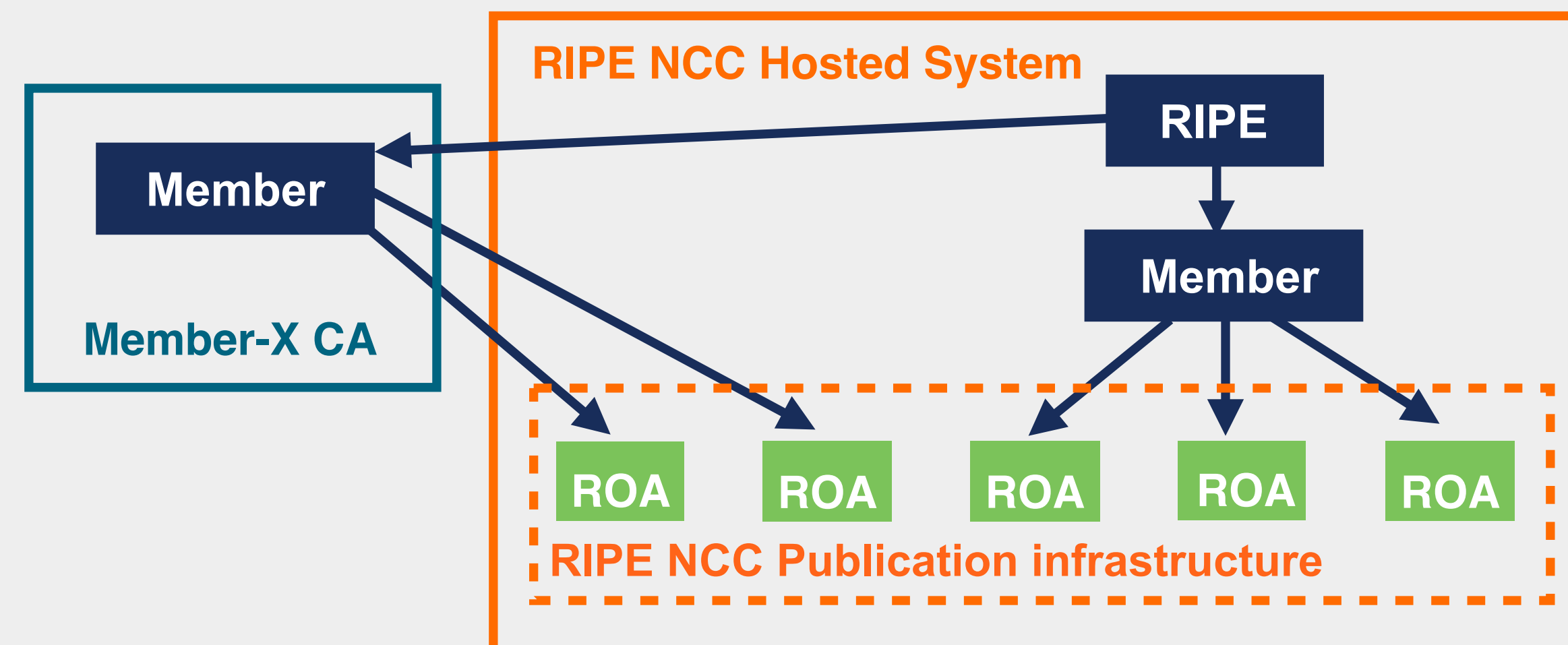
Coming soon: ASPA

- Autonomous System Provider Authorisation

- Validation of AS_PATH

  - "AS_PATH verification provides detection and mitigation of route leaks and improbable AS paths. It also to some degree provides protection against prefix hijacks with forged-origin or forged-path-segment" - from IETF draft

- Current support:

  - By a couple of validators

  - Supported by RIPE NCC's API in pilot environment (planned in portal)

  - RPKI-to-Router support — RFC 8210bis, final draft

  - OpenBGPD and NIST BGP-SRx

Promoting Route Origin Validation (ROV)

- Plan to promote ROV within Tier 1 providers

- Very early stage
  - Measure ROV level using RoVista
    - https://rovista.netsecurelab.org/
    - https://labs.ripe.net/author/tijay-chung/help-validate-rov-adoption-measurements-from-rovista/
 - Monitor ROV adoption

- Check your AS!

RoVista | Home | Contacts

RoVista

RoVista measures the RoV filtering ratio of network operators. This ratio is derived from our measurement technique that uses (1) in-the-wild invalid BGP Prefixes and (2) IP-ID side-channel technique. The details will be published soon.

ROV Filtering Ratio

total   ratio   filter   remove

Sunday, Jul 24, 2022
total: 59
ratio: 1
filter: 59
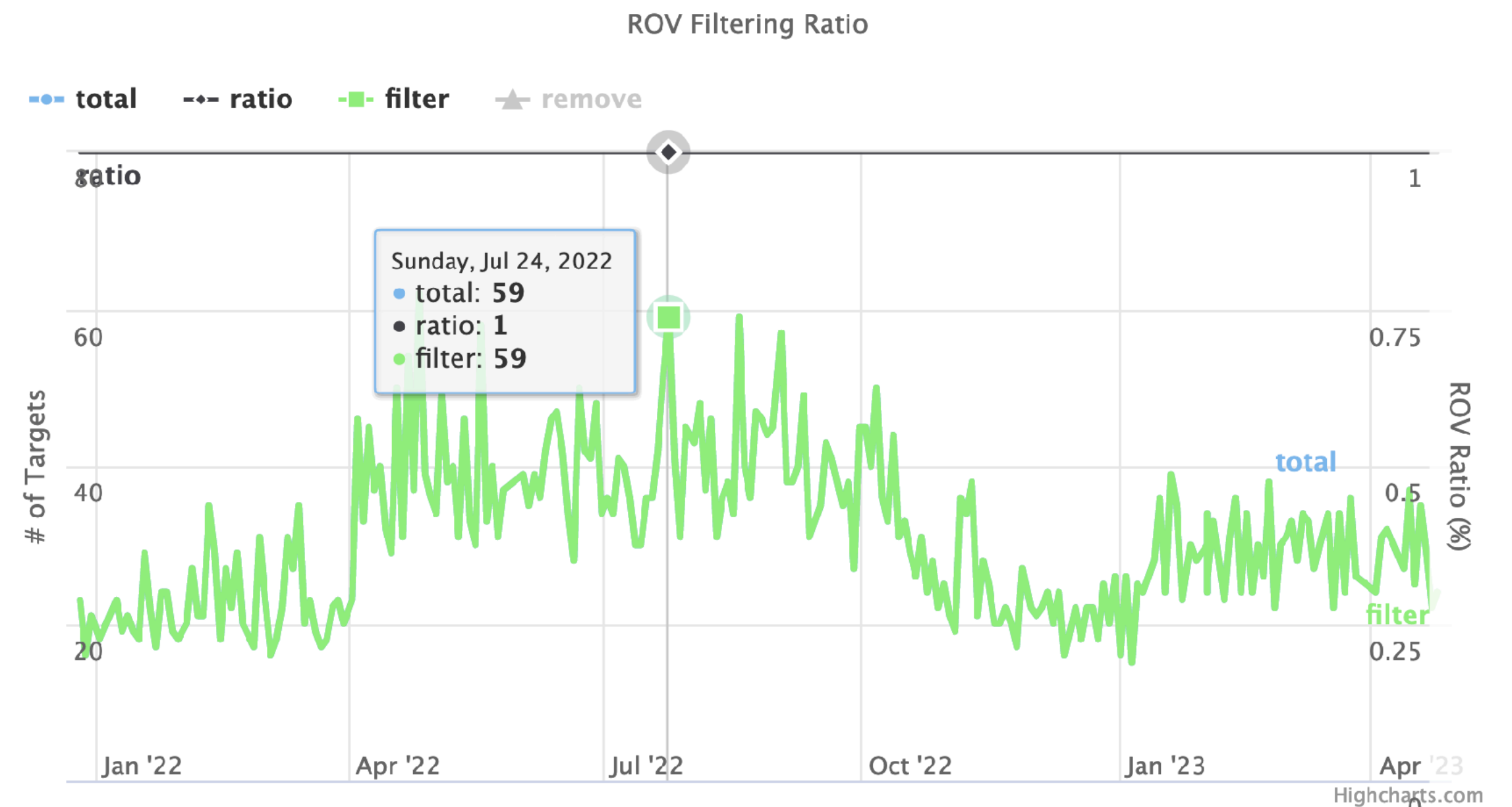
The Internet Routing Registry (IRR)

Near Real Time Mirroring (NRTM)

IRR: NRTM v4

- Near Real Time Mirroring (NRTM)

- Protocol for IRR mirroring

- HTTPS, JSON + RPSL

- Periodic Snapshot Files and regular Delta Files

  - Inspired by RRDP

- Improved scalability

- Get involved!

  - https://github.com/mxsasha/nrtmv4/blob/main/draft-ietf-grow-nrtm-v4.txt

  - email the authors, db-wg@ripe.net

Summary

- RPKI has become a mature ecosystem

- Use RPKI, in whichever mode fits your case

- ROV + ASPA can prevent a large fraction of hijacks and route leaks

- Check RoVista to see details for your network

- Get involved with NRTMv4

Join us at

RIPE 86

Rotterdam, Netherlands
22 – 26 May 2023

Questions

theodoros.polychniatis@ripe.net
rpki@ripe.net