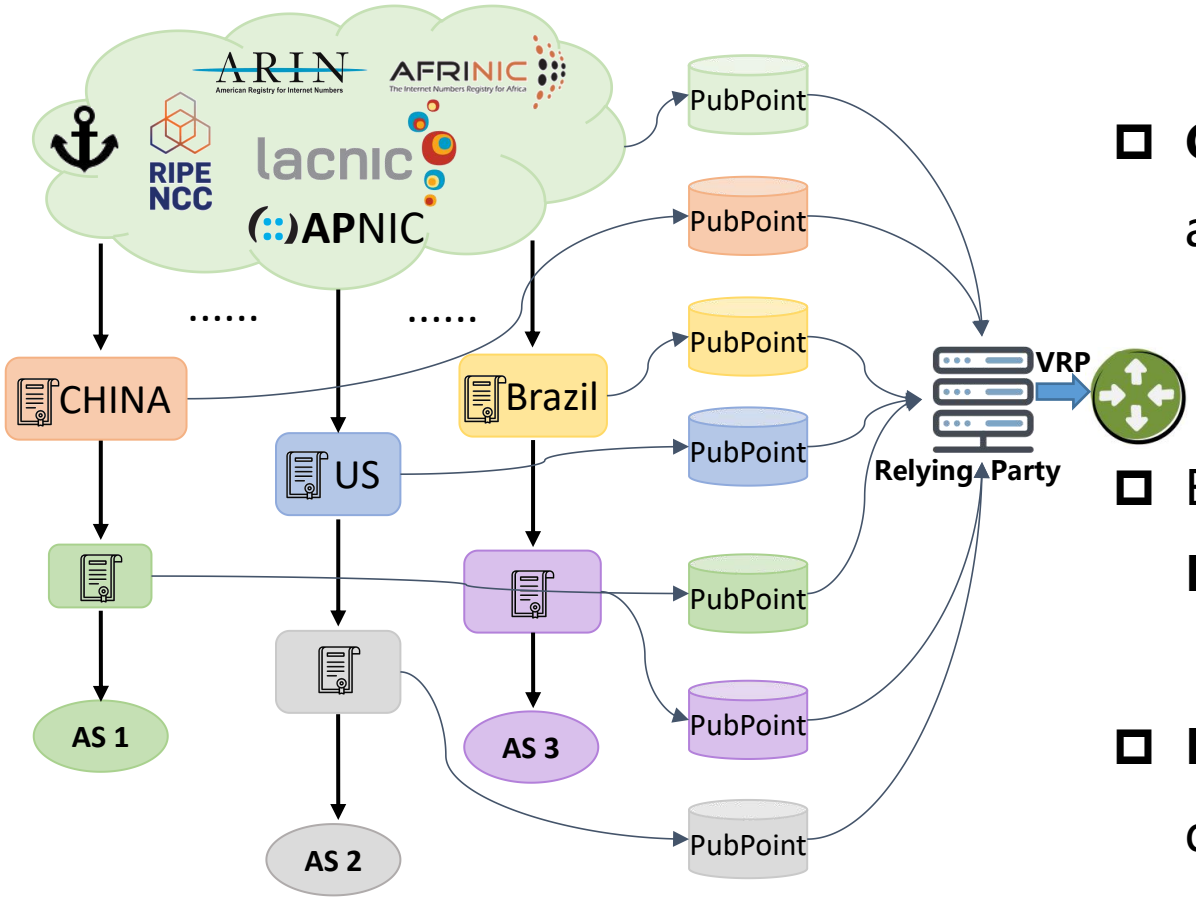
RPKI Repository Problem Statement and Analysis

draft-li-sidrops-rpki-repository-problem-statement-00

Dan Li, Li Chen, **Yingying Su**
ZGC lab & Tsinghua university

November, 2024

RPKI Repository Architecture



Hierarchical Architecture of RPKI

- **CA or RPKI authority** can issue **Resource Certificate (RC)** and **Route Origin Authorization (ROA)** to **INR holder**
  - RC → reallocate INRs
  - ROA → authorize ASes to originate specific IP prefixes
- Each CA will upload RPKI objects it signs to the **Publication Point (PP)** it operates or designates
  - These PPs collectively form the **RPKI Repository**
- **Relying Parties (RP)** periodically traverse all PPs, download and validate all RPKI objects
  - Generate **Verified ROA Payloads (VRPs)** to help border routers make routing decisions

RPKI Repository Design Leads to Three Problems

P1. Vulnerable to Single Point of Failure

- Each CA stores the **RPKI objects** it issues **in the unique PP** it runs or designates
- Any PP' s **failure** will **hinder RPs** from obtaining **complete** RPKI object views

P2. Poor Scalability

- RP local cache refresh involves **traversing all PPs** to fetch updated data
- The number of PPs and RPs are expected to **increase** with the further deployment of ROA and ROV

P3. Unilateral Reliance on RPKI Authority

- RPKI Repository is not **tamper-resistant**, authorities can **unilaterally undermine** any RPKI objects **without consent** from subordinate INR holders.

The problems will affect the **integrity** and **accuracy** of the stored RPKI objects and hinder future large-scale RPKI deployment!

P1. Vulnerable to Single Point of Failure

- Repository PP deployment (63 independent repositories)
  - Only **9** out of **63** PPs are hosted in **CDNs**
    - **8** in cloudflare' AS13335, **1** in Amazon' AS16509
  - **60** PPs are hosted in a single AS (for RRDP)
    - The availability of these PPs is highly dependent on the reachability of a single AS
  - **14** PPs carry the ROAs of the ASes where they are located
    - Introduce unwanted **interdependence** between the **accessibility** of a PP and the **reachability** of the PP' s AS

Real-world incidents of PP

JPNIC

Service outage: ROAWeb and RPKI repository (resolved)

Service outage: Disk full caused lost ROA validity

APNIC

Service Announcement: RPKI Outage

RIPE NCC RPKI Outage on 23 June 2022

....

[1] discovered a large and persistent amount of networking errors in RPKI Repository, including unreachability, unstable connections, and DNS issues; PP blackouts affect ROV, PPs require high availability and network stability; our measurement shows that due to network instability, the time for RPs to refresh the local cache ranges from 64s to 650s (1600 rounds)

unavailable objects and slowing down the fetching of RPKI objects for all globally running RPs

Any **single point of failure** in PPs may **hinder** RPs from obtaining **complete RPKI object views**!

[1] Donika Mirdita et al. SoK: An Introspective Analysis of RPKI Security, usenix security 2025

P1. Vulnerable to Single Point of Failure

The existing solutions in current RPKI are **good** but **insufficient…**

- Two access protocols--RRDP & RSYNC
  - Only **8** repositories' RRDP server and rsync server are hosted in different ASes
  - At least **20%** of RPs did not obey the standard and would not fall back to rsync when RRDP fails [1][2].
- Cached data is available
  - Cached data is prone to becoming invalid in prolonged outages, especially for critical data with shorter validity periods, such as manifests (Over **50%** of manifests have a validity period of less than **24 hours**)
  - Using cached data to validate BGP updates increases the ROV inaccuracy

[1] Donika Mirdita et al. SoK: An Introspective Analysis of RPKI Security, usenix security 2025
[2] Kristoff J, On measuring RPKI relying parties. IMC 2020

P2. Poor Scalability

The current practice of delegated RPKI will lead to an increase in the number of independent repository instances

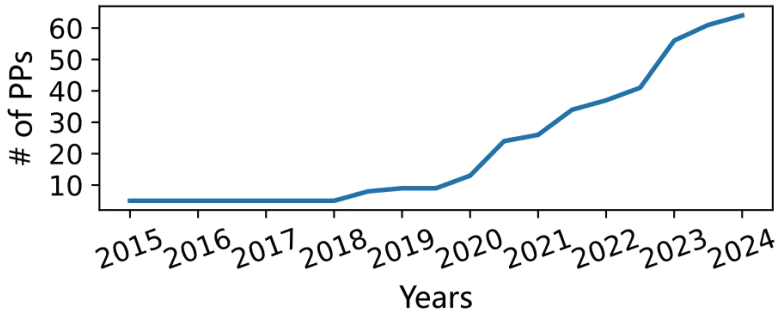
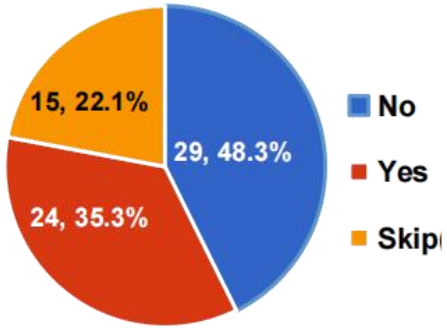


Fig. thce number of PPs over 10 years.



Q: Will you consider using delegated RPKI and running your own PP in the future? (w/ROA).

- The number of PPs has grown more than 12 times
  - from 5 PPs run by RIRs to more than 60 PPs
- Randomly sent a questionnaire to 2,500 ROA deployer, out of 68 responses, 24 said they would consider running their own PPs in the future
- If ROA is fully deployed, the number of PPs will reach **10k** [Hlavacek et.al, sigcomm 2023]

P2. Poor Scalability

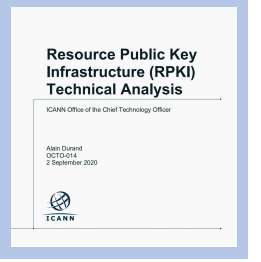
Potential problems

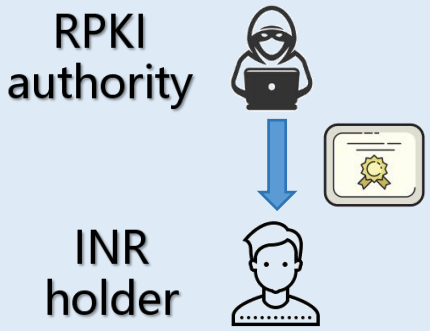
- Threaten the scalability of RPKI
  - With the further deployment of ROA and the rise of delegated RPKI, there will be **more and more PPs**; And with the further deployment of ROV, there will be **more RPs**.
- Increase the cost of RP refreshing
  - RPs will need to access more PPs, and PPs will need to serve more RPs.
  - The increase in the number of **bidirectional connections** will **increase the cost of RP refreshes**.
- PPs with unwanted purposes will bring unexpected risks to RPs
  - A series of work[1-5] has demonstrated the feasibility of using delegated RPKI to exploit vulnerabilities in RPKI protocol or in RP software implementations to stall RPs or crash them.
  - New attack vectors are on the way, it is difficult to prevent the risk fundamentally……

[1] Donika Mirdita, et al. Poster: RPKI kill switch. CCS 2022
[2] Van Hove, Rpkiller: Threat analysis from an RPKI relying party perspective 2022
[3] Tomas Hlavacek, et al. Stalloris: RPKI Downgrade Attack. usenix security 2022
[4] Tomas Hlavacek, et al. Beyond Limits: How to Disable Validators in Secure Networks. sigcomm 2023
[5] Donika Mirdita, et al. The CURE to Vulnerabilities in RPKI Validation. NDSS 2024

P3. Unilateral Reliance on RPKI Authority

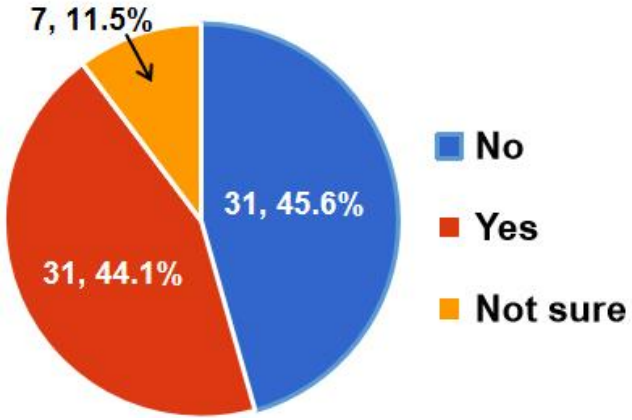
- RFC 8211
- RPKI Technical Analysis (ICANN 2020)





Malicious actions by RPKI authority

Unilateral deletion, revocation, corruption, modification RPKI objects diminish the set of INRs associated with the INR holder



Q: Are you worried that RPKI authorities maliciously compromise your certificates, which could affect the legitimacy of your BGP updates? (w/ROA)

☐ Real-World Concerns

- 44.1% of the AS operators have expressed concerns about malicious authorities
- One operator considers the threat from authorities to be the most serious problem
- Two operators had lost all their ROAs due to administrative/human reasons

P3. Unilateral Reliance on RPKI Authority

The existing solutions in current RPKI are **good** but **insufficient...**

- RPKI historical data tracking tools [1-3]
  - Tools cannot form a complete and consistent RPKI view
  - These tools can only be used for performing audits after the fact
- Changes CA
  - It is difficult for INR holders to rent IP from another CA quickly enough and migrate network services from one IP prefix to another
- RFC 8181
  - RPKI authority can separat CA engine and operations of repository functions
  - However, the choice of which repository to use is still designated by the RPKI authority, and operations on RPKI objetcs stored in the repository PP are also performed by the RPKI authority.

[1] https://ftp.ripe.net/rpki/,
[2] http://www.rpkiviews.org/
[3] https://delta-rpkilines.nlnetlabs.net/

Desired properties

New RPKI Repository Architecture

- **0. Compatibility**
  - No modification to RPKI hierarchical certificate issuance architecture
  - Be compatible with current RPKI Repository architecture and support incremental deployment...
- **1. Availability**
  - Distributed data storage, enable a single RPKI object to be backed up across multiple repository nodes
  - The integrity of the RPKI data accessed by RPs will not be affected even if a single PP experiences a point of failure...
- **2. Scalability**
  - Prevent unlimited growth of the number of PPs
  - Ensure timely updates of RPKI data to RPs
- **3. Security & Auditability**
  - Actively defend against RPKI authorities' malicious behavior
  - Maintain a complete and consistent RPKI historical data view, provide audit function for RPKI

Summary

- RPKI reliability/scalability/security analysis from the perspective of RPKI Repository
- The desired properties for a future RPKI Repository

Thanks!

Q & A