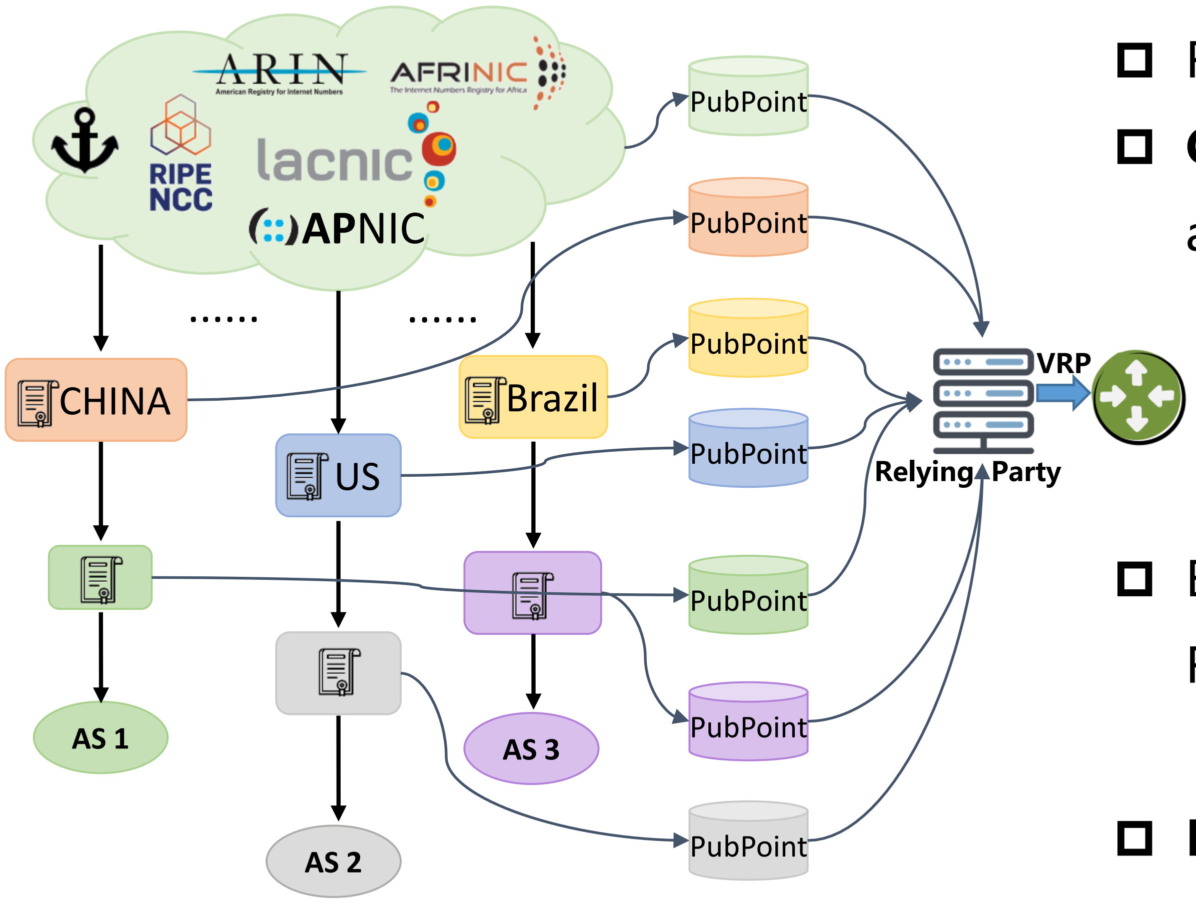
dRR: A Decentralized, Scalable, and Auditable Architecture for RPKI Repository

Yingying Su, Dan Li, Li Chen, Qi Li and Sitong Ling
Tsinghua university

February, 2024

Resource Public Key Infrastructure



Hierarchical Architecture of RPKI

- □ RPKI is standardized by **IETF** to prevent **prefix hijackings**
- □ **CA or RPKI authority** can sign **Resource Certificate (RC)** and **Route Origin Authorization (ROA)** to **INR holder**
  - ➢ RC → reallocate INRs
  - ➢ ROA → authorize ASes to originate specific IP prefixes
- □ Each CA runs a **Publication Point (PP)** to store RCs and ROAs issued for INR holders
  - ➢ All 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. Unilateral Reliance on RPKI Authority

- □ RPKI Repository is not **tamper-resistant**, authorities can **unilaterally undermine** any RPKI objects **without** INR holders' **consent**

P2. Vulnerable to Single Point of Failure

- □ Any PP's **failure** will **hinder RPs** from obtaining **complete** RPKI object views
- □ Introduce **interdependence** between the **accessibility** of a PP and the **reachability** of the PP's AS

P3. Poor Scalability

- □ RP local cache refresh involves **traversing all PPs** to fetch updated data
- □ The number of PPs is expected to **increase dramatically** with the further deployment of ROA

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

Data-driven Threat Analysis

- The first data-driven threat analysis for RPKI Repository

P1 and P3 → ***Worldwide Survey***

P2 → ***RPKI Repository Measurement***

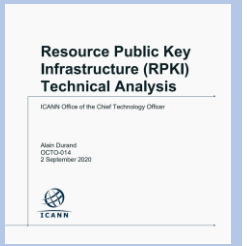
P1. Unilateral Reliance on RPKI Authority

Malicious actions by RPKI authority

Unilateral deletion, revocation, corruption, modification

- RFC 8211

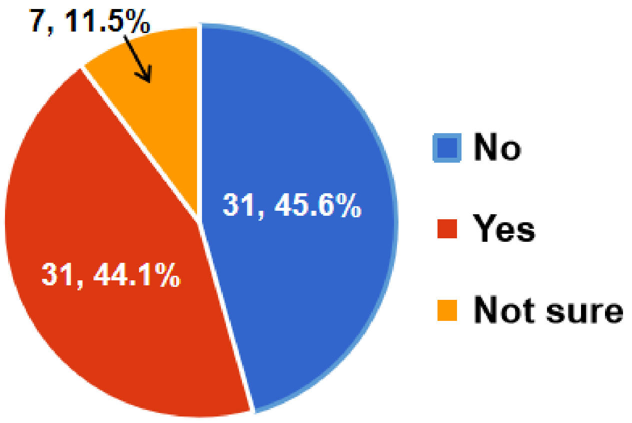
- RPKI Technical Analysis (ICANN 2020)



Resource Public Key Infrastructure (RPKI) Technical Analysis

ICANN Office of the Chief Technology Officer

Alain Durand
OCTO-014
2 September 2020



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

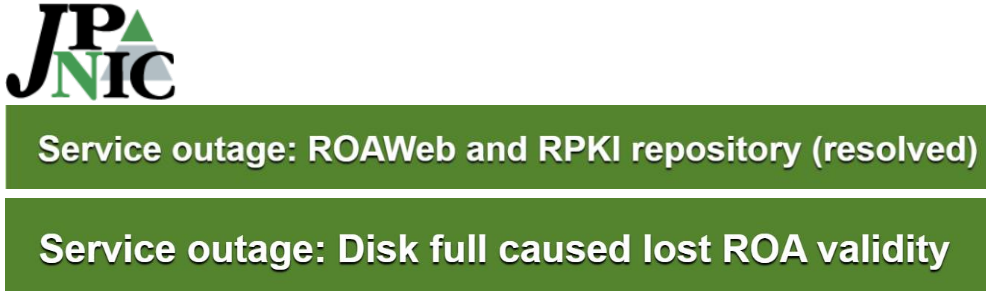
- 44.1% of the AS operators expressed concerns about malicious authorities
- One operator considers the threat from authorities to be the most serious problem
- Two operators had lost all their ROAs due to administrative/human reasons

P2. Vulnerable to Single Point of Failure

□ CDN deployment

- Only **8** PPs are hosted in **CDNs**
  - **7** in cloudflare’ AS13335, **1** in Amazon’ AS16509
- **58** PPs are hosted in a single AS
  - The availability of these PPs is highly dependent on the reachability of a single AS
- **14** PPs carry the ROA of the ASes they located
  - The accessibility of PPs will form a circular dependency on the reachability of ASes

Real-world incidents of PP



Service outage: ROAWeb and RPKI repository (resolved)

Service outage: Disk full caused lost ROA validity

Service Announcement: RPKI Outage

RPKI Outage on 23 June 2022

....

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

P3. Poor Scalability

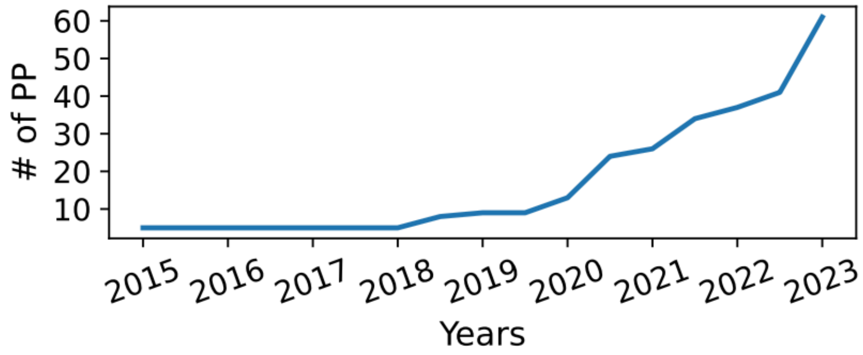
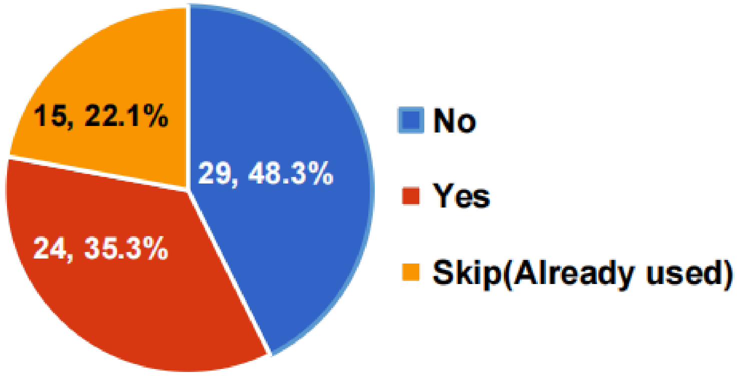


Fig. thce number of PPs over 9 years.

- The number of PPs has grown more than 12 times
- Many AS operators consider running PPs
- If ROA is fully deployed, the number of PPs will reach **10k** [Hlavacek et.al, sigcomm 2023]



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

potential problems

- Threaten the **scalability** of RPKI
- Increase the **cost** of RP refreshing
- Bring unexpected **risks** to RPs

key Idea of dRR

Separating RPKI object distribution from signing!

- Decouple PP and RPKI Authority
- Design a third-party repository for RPKI → **dRR**

Design Goal of dRR

dRR means Decentralized RPKI Repository

For P1

- □ Defend against RPKI authorities' malicious behavior
- □ Allow RPs verify certificate status
- □ Allow INR holders verify the integrity of RPKI views
- □ RPKI historical data can be audited

For P2

- □ Defend against single points of failure
- □ Truly distributed data storage
- □ PP accessibility is independent of AS accessibility

For P3

- □ Prevent unlimited growth in the number of PPs
- □ Improve the reliability of RPKI Repository system

Be **compatible** with RPKI architecture and supports **incremental** deployment

CS federation

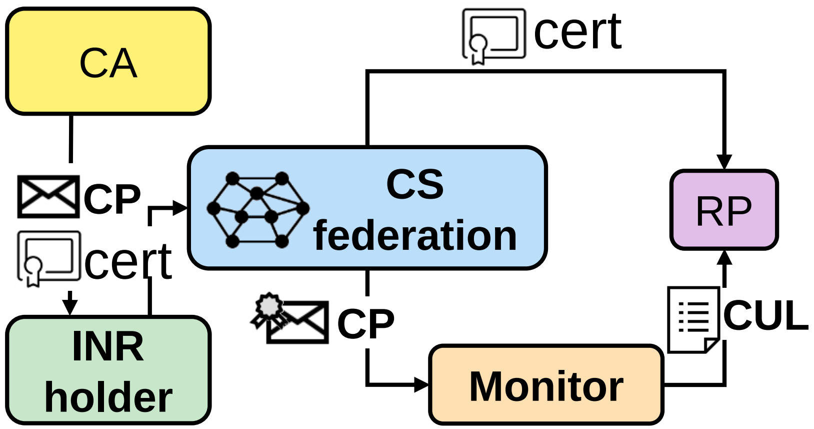


Fig. dRR architecture

VS

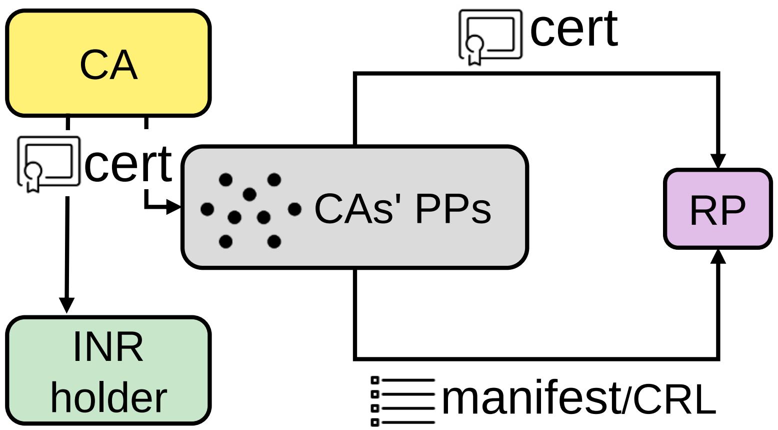


Fig. current RPKI Repository

Key new entitiesfor dRR: *CS federation* and *Monitor*

dRR Workflow

dRR new entity

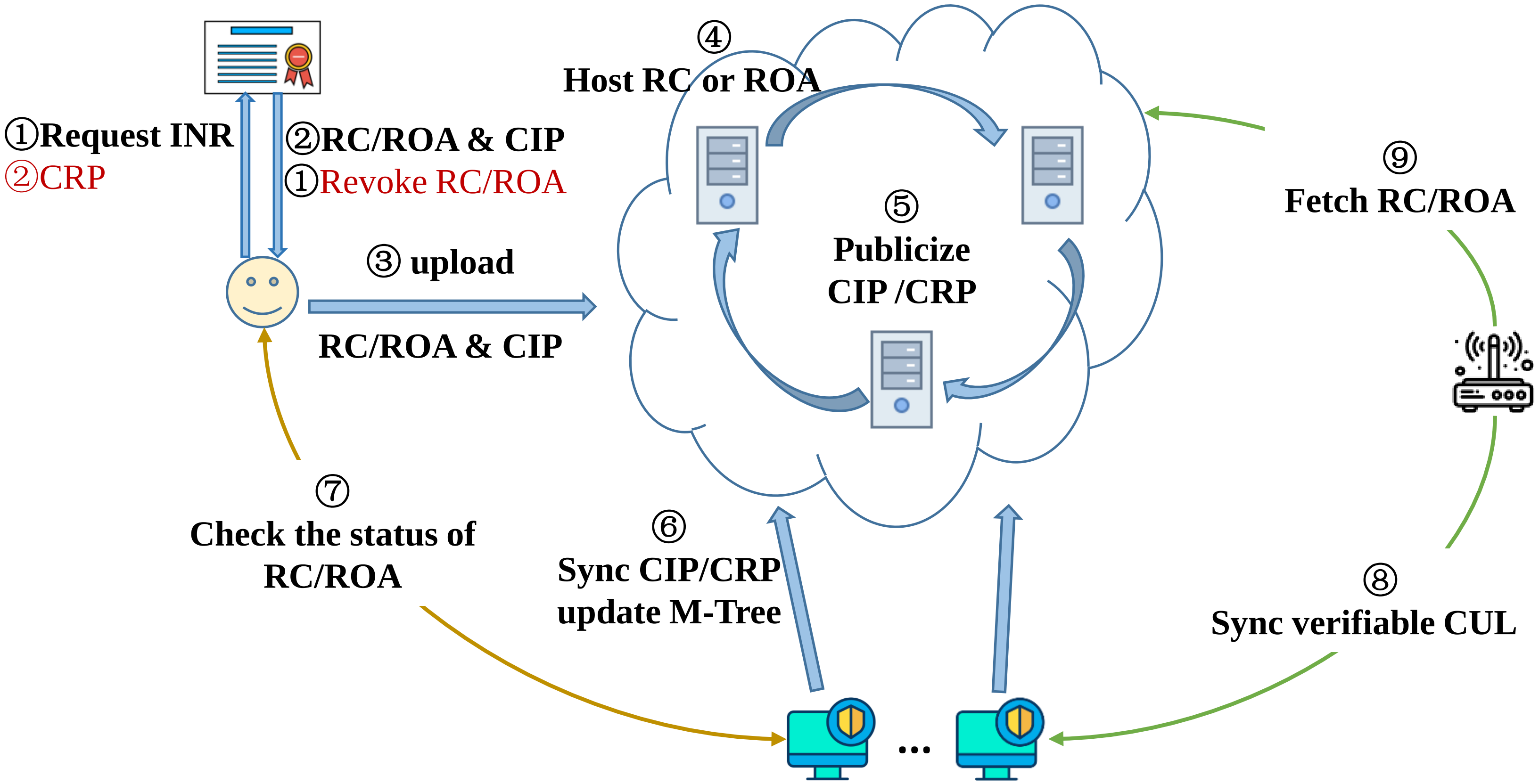
- Cert Server (CS)
- Monitor

dRR new data structure

- Certificate Issuance Policy (CIP)
- Certificate Revocation Policy (CRP)
- Certificate Update List (CUL)
- M-Tree

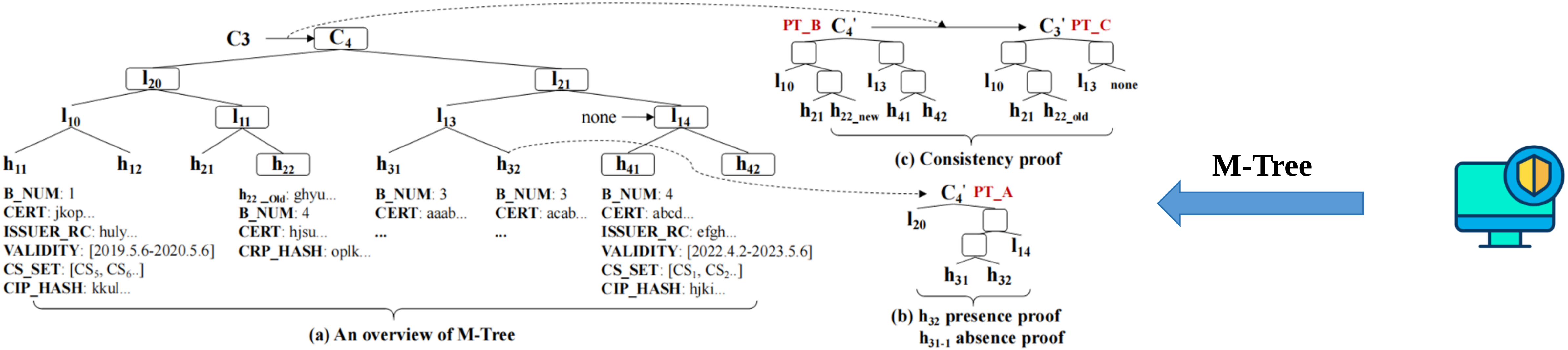
RPKI entity

- INR holder
- RPKI Authority
- Relaying Party



Monitor

- Monitor
  - Fetch CIP/CRP， updates M-Tree
  - Server RPs: provide verifiable CUL for RPs
  - Serve INR holders: allow RPs verify certificate status



(a) An overview of M-Tree

(c) Consistency proof

(b) h_{32} presence proof
$h_{31\text{-}1}$ absence proof

dRR

For P1：

- INR holders can freely select trusted CSs to hoste RC/ROA
- CIPs and CRPs provide a trusted RPKI historical ledger
- M-Tree meet the security requirements of RPs and INR holders

For P2：

- One certificate can be hosted on multiple CS nodes

For P3：

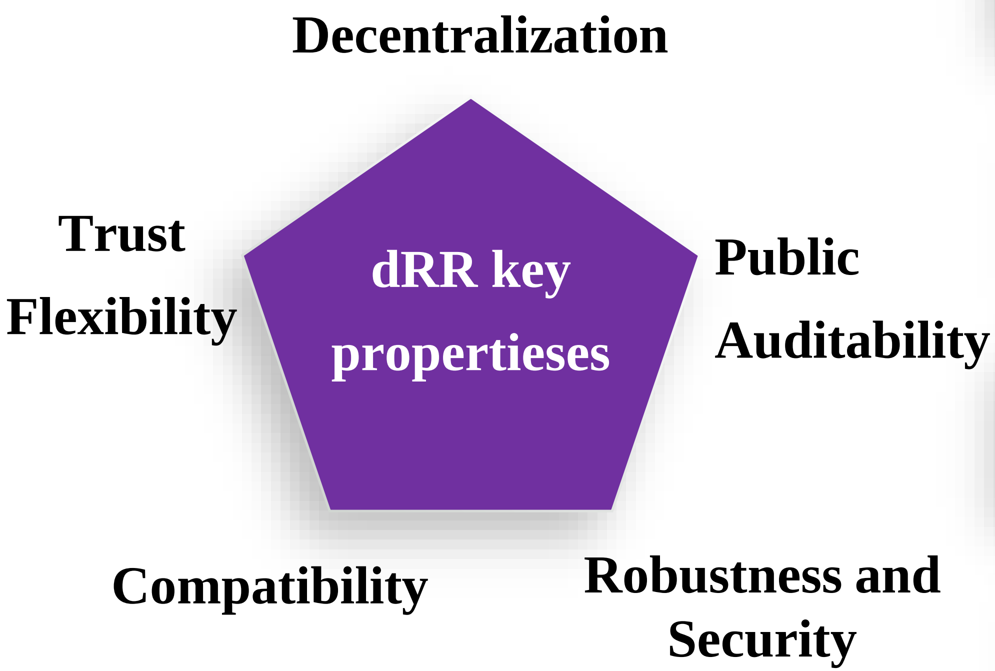
- The access mechanism effectively limits the number of CS nodes

Who can be CS nodes or monitor?

⇩

State-run institutions and large ISPs (e.g.,Akamai, Amazon, Cloudflare, etc.) that have reliable service infrastructure, such as CDNs and good reputation

Key Properties of dRR



Decentralization

Balance the disproportionate power between RPKI Authority and INR holders

Trust Flexibility

INR holders & RPs can freely choose CS or Monitor to meet their needs

Public Auditability

All historical data is publicly auditable

Robustness & Security

dRR is more robust and secure than current RPKI repository

Compatibility

dRR is compatible with RPKI architecture

Evaluating dRR on a Global Testbed

Global Testbed

- 100 server nodes across 15 countries
- 50 nodes for CS, 50 nodes for Monitors

Two performance metrics

- The throughput of the CS federation
- The additional latency introduced by dRR

Evaluating dRR on a Global Testbed

- **Baseline**: certificate renewal peaks at 60k/day
- CS federation
  - Hotstuff Consensus protocol
  - 50 CS nodes， the throughput reachs 300+/s, 450 times the peak value
  - The delay introduced is less than 2s
- Monitor
  - The delay introduced by is less than 0.5s
  - The bottleneck is certificate signing/synchronization, which takes tens of minutes to several hours

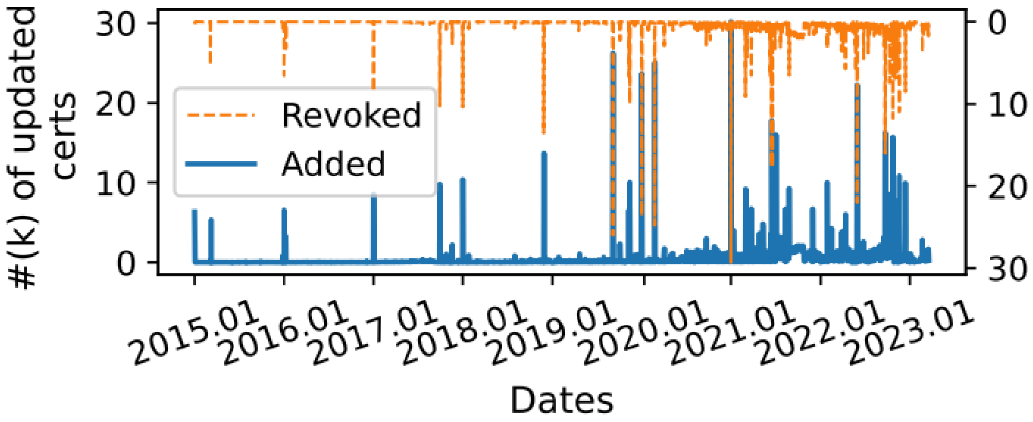


Fig. current certificate Update Frequency

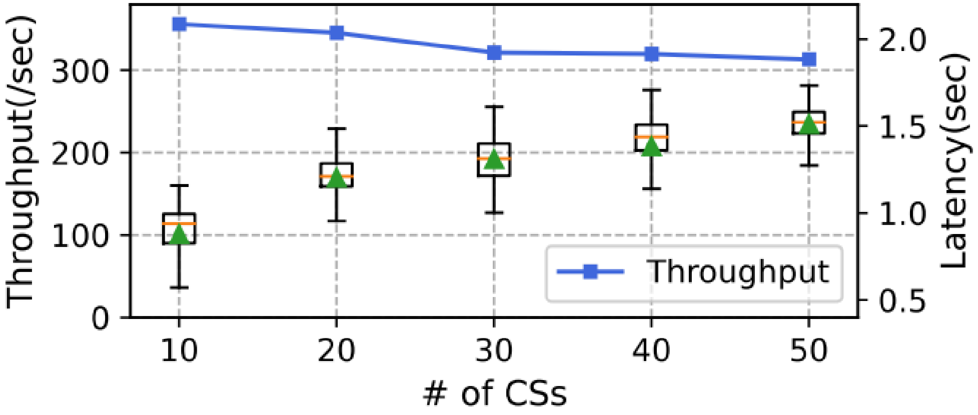


Fig. the throughput and delay of CS federation

Summary

- □ The fisrt data-driven RPKI threat analysis
- □ The first RPKI-compatible architecture designed to enhance the current vulnerable RPKI Repository
- □ Implement a prototype of dRR and evaluate it on a global testbed with 100 nodes
- □ Potential benefits: resist mirror world attacks...

Thanks!

Q & A