Poster: Exploring the Landscape of RPKI Relying Parties

Donika Mirdita
TU Darmstadt
ATHENE
Darmstadt, Germany

Haya Schulmann
Goethe-Univ. Frankfurt
ATHENE
Darmstadt, Germany

Michael Waidner
TU Darmstadt
ATHENE
Darmstadt, Germany

Abstract

The Resource Public Key Infrastructure (RPKI) is the most successful routing defense mechanism currently deployed throughout critical Internet infrastructures around the world. According to recent works, RPKI deployment boasts over 55% global prefix resource coverage, and at least 27% global protocol enforcement; all this success over a short period of time.

In this work, we investigate for the first time deployment trends of the Relying Party (RP), the RPKI component responsible for collecting and enforcing RPKI on routers. We map RP locations, deployment parameters, vulnerability distributions, and describe the evolution of deployment trends over two measurement periods three years apart. Through this exploratory analysis, we map global patterns and the preferred deployment configurations by network operators. We observe how within three years, RP traffic increased by 45%, while 89% of traffic stems from one software type. Our measurements show a strong preference by operators to self-host, coupled with inadequate rates of RP vulnerability mitigation.

CCS Concepts

• **Security and privacy → Network security**.

Keywords

BGP, RPKI, Relying Party

ACM Reference Format:
Donika Mirdita, Haya Schulmann, and Michael Waidner. 2025. Poster: Exploring the Landscape of RPKI Relying Parties. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3719027.3760721

1 Introduction

The Border Gateway Protocol (BGP) is the defacto inter-domain routing protocol. It was designed at a time when security was not a priority. As a result, standalone BGP is vulnerable to hijacks and route leaks. The RPKI was first introduced two decades after BGP's standardization. It outperformed existing routing security solutions and became the primary security wrapper for BGP. RPKI deployment trends and industry adoption rates are promising, eclipsing other proposals [1, 2]. Over 55% [3] of globally announced prefixes are covered by RPKI, and at least 27% [4] of operators enforce it as of 2022, a number that is higher today due to more Tier-1 providers and Internet Exchange Points (IXPs) joining the RPKI ecosystem after the original measurements. This success led the U.S. government to take notice of RPKI and issue guidelines [5, 6] to encourage RPKI adoption throughout the nation's digital infrastructure.

The RPKI consists of two software suites: repositories serving and RPs collecting and cryptographically validating prefix ownership information, otherwise known as Route Origin Authorizations (ROAs), see Figure 1. The RP acts as the middleman between repositories and BGP routers. RPs send the validated ROA payloads to routers, which proceed to use this information to run Route Origin Validation (ROV). ROV is the process by which the router validates the correctness of the origin ASN of route paths received via BGP Announcements. If a route's origin matches a ROA, it is considered valid; if a route's origin differs from a ROA, it is marked as invalid. Finally, if there is no ROA coverage for a route, the fail-open algorithm treats it as valid.

There is an abundance of research on RPKI. Existing work focuses on analyzing RPKI vulnerabilities [7–9] and ROV enforcement rates [4, 10, 11]. Current research on RPs focuses primarily on the analysis of RP behavior and synchronization [12, 13]. The modus operandi of RPs, and the reliance of routers on their availability and correctness to enforce RPKI in the first place, suggests that RP deployment strategies, types, networks, and availability are of the outmost importance for RPKI health.

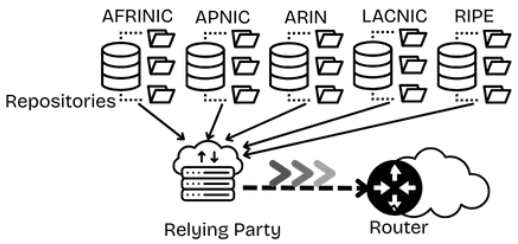

Figure 1: Resource Public Key Infrastructure

Contributions: While the RPKI research landscape is rich, no prior work has addressed the open questions of RPKI validator deployment trends and configurations, geographic distributions, cluster heterogeneity, vulnerability distribution, and management preferences for network operators. RPKI validators are flexible enough to be deployed on-premise or outsourced to external cloud providers, an important characteristic that allows for various deployment architectures. In this poster, we present the first exploratory measurements of RPKI deployment characteristics, and we extend our analysis across two time periods 3 years apart to capture the evolution of RPKI validator deployments over time.

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3760721

Window	Unique IPs	Unique Networks	Countries	RP Redundancy	RPs on Cloud	Vuln. Status
1.07.2022	2,587	1,851	100	13.8%	no data	31.8%
1.07.2025	5,775	3,597	126	14.2%	4.4%	43%

Table 1: Relying Party Deployment Statistics

Window	Routinator	rpki-client	fort	OctoRPKI	RIPE NCC Validator	other
1.07.2022	74.6%	7.3%	2.5%	8.3%	6.5%	0.8%
1.07.2025	67.6%	25.9%	3.2%	1,65%	0.3%	1.35%

Table 2: Relying Party Implementation Distribution, in %

2 Evaluations

We set up a dedicated repository under RIPE. RPs regularly query the full RPKI tree, including our repository, thus allowing us to collect their metadata. We collect this data over a multi-year period. In this work, we compare two equidistant 24h windows on July 1st 2022 and 2025. We use [14, 15] to extract network information, geograhic location, origin ASN, and legal ownership for the actively observed RP instances. We summarize our data in Tables 1 and 2.

RP Traffic. We quantify the incoming RP traffic for both measurement windows. During our 24h measurement window in 2025, our repository received 467,482 requests compared to the 320,785 requests during the measurement window in 2022, marking a 45% uptick in traffic. We observe a 123% increase in unique IPs and 94.3% in unique networks. This increase in RP deployment and traffic, correlates with a 41% increase in global ROA coverage, up from 39% to 55% according to NIST [3], see Table 1. Table 2 shows the software distribution of RP implementations during our two measurements. In 2025, Routinator is the most popular RP, followed by rpki-client and fort. Routinator has a 10 minute refresh interval in its default configurations, a timer which remains often unchanged by deployers, therefore 89% of all traffic towards our repository stems from this RP implementation.

RP Deployment Strategy. RPKI is still going through early adoption pains. The RP is the engine of the infrastructure and a service that requires high availability, therefore we pose two questions on RPKI deployment preferences, namely:
① Do RPKI deployers employ redundancy to ensure RP availability?
② Where do RPs get primarily deployed: on-premise or remotely?

RP Redundancy. We fingerprint RPs by their full agent header per unique network location. In 2022 and 2025, there are 256 and 512 unique networks, respectively, hosting more than one RP at a time. We analyze the top 30 networks with heterogeneous RP deployments. We identify the networks with the most unique RP deployments (4–7 different fingerprints) to be important Internet companies like Juniper, RIPE NCC, LEVEL3, COGENT, and other major global Internet Service Providers (ISPs) and IXPs. With few exceptions, RP deployment sets are heterogeneous, meaning deployers use different RP implementations for operational robustness: if one RP type is attacked and incapacitated, other RPs can step in. However, we notice that even in 2025, major Internet backbones are running discontinued or outdated RPs with known vulnerabilities alongside few modern up-to-date RP versions. Throughout 2025, we observe a slight increase in browser-based requests. Browsers are unsuitable for using RPKI in production, suggesting either exploratory work on infrastructure or newly developed browser-based apps to parse RPKI data. Browser-based queries often came from web-hosting networks. Additionally, we observe the first attempt at trying to fuzz (and therefore attempting to crash) a live repository. The query is associated with the agent header of an open source fuzzer "Fuzz Faster U Fool v2.1.0-dev."

RP Location. We investigate RP deployment locations. RPs can either be deployed on-premise or outsourced to the cloud. Since network ranges for cloud operators change over time, we can evaluate only the 2025 data. We compare the cloud-provider-ip-addresses-dataset[1] with our 2025 data and find that at least 4.4% of RPs are hosted on verified cloud providers. Namely, we find RPs included in the IP ranges of Google Cloud (8), AWS (35) and Azure (154).

Deployment Vulnerabilities. Throughout the two measurement windows, 31.8% and 43% of RPs respectively were affected by known vulnerabilities at the time of collection. Our data suggests that new entities entered the RPKI ecosystem using the latest software versions, while legacy deployments continue using outdated software. Unpatched software still runs on internal networks of important companies. By 2025, RIPE NCC Validator and OctoRPKI have been discontinued since 2022 and 2023 respectively, but we still see them in the wild, sometime within the internal networks of ISPs and IXPs. If these networks are not hosted on the cloud, we can surmise that these outdated RPs might still be used in production.

Geographic Spread. Figure 2 is a heatmap of unique RP request rates per country. The size of the red bubble is proportional to the number of unique vulnerable or discontinued RPs. Most requests come from North America, Brazil, Europe and mainland Asia. This geographic distribution matches to some extent ROV enforcement rates[2]. Joining the RPKI as an ROV enforcer often comes hand in hand with entering your own resources for ROA coverage. Noticeably, Europe, North America and Asia are covered by RIPE NCC, ARIN and APNIC Regional Internet Registries - 3 entities that offer streamlined and independent access to the RPKI-tree as opposed to the heavily centralized management of LACNIC and AFRINIC for South America and Africa respectively. We observe that most vulnerable RPs reside primarily in countries with extensive RPKI deployment, suggesting that vulnerable infrastructures persist due to neglect, and are not the result of a poor choice during initial setup.

[1] https://github.com/rezmoss/cloud-provider-ip-addresses
[2] https://stats.labs.apnic.net/rpki

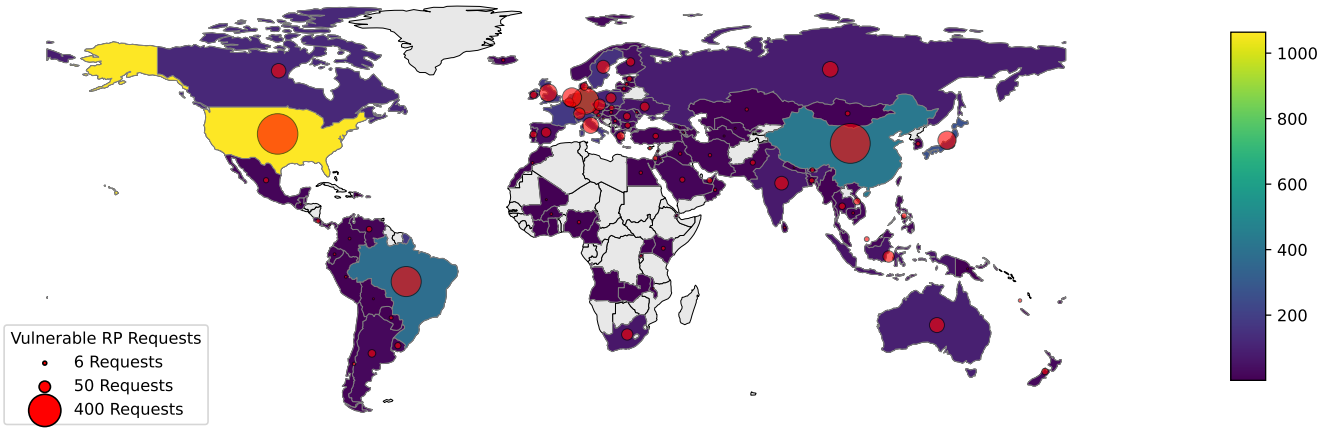

Figure 2: Heatmap of RP Geographic Distribution, 2025

3 Analysis and Future Work

Given the increasing importance of RPKI and the outsource-able nature of its components, we analyze deployment trends in order to gauge preferences and identify potential problems. RPs are vital software that require high availability, however they are vulnerable to native attacks and software bugs are ever present. Since all RPKI-enabled routers can connect to multiple RPs, the use of multiple heterogeneous RP deployments per operator should be the standard. While serious operators are doing just that, they are diminishing their security returns by running outdated software with known vulnerabilities. Since few RPKI enforcers use cloud providers to host RPs, many of these outdated and vulnerable services are located within internal networks and potentially have a direct connection with BGP routers. Additionally, we observe that traffic is increasing disproportionally faster than RPKI adoption rates, which can be partially traced back to arbitrary default configurations of some RP implementations. All of this points to RP deployers not being security- and configuration-aware. Such attitudes lead to increased attack surfaces and repository overload. From a geographic perspective, RP deployment roughly correlates with ROV enforcement. However, there are more decisive factors that influence ROV coverage, such as the size and importance of participating operators, and total network prefix space of the area.

This brings us to future work. Longitudinal measurements over contiguous long periods of time are needed. Some locations are not represented in our 24h window RP dataset even though other work shows there is some ROV enforcement there. This could be the result of ROV enforcement by external upstream providers, RP outsourcing to cloud providers with networks registered in other jurisdictions, or networking bottlenecks preventing us from getting some RP requests for a short time period. To answer these questions, additional longform analysis of RP deployments and flexible, efficient RP-to-ROV correlation strategies are necessary. Another aspect requiring further work is the compiling of more inclusive cloud operator prefix datasets, which should include smaller service providers, thereby alongside ROV correlations, improving the accuracy of RP cloud outsourcing measurements.

Acknowledgements

This work has been co-funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) SFB 1119.

References

[1] IRR. Internet Routing Registry. https://www.irr.net, 2025.
[2] Geoff Huston and Randy Bush. Securing bgp with bgpsec. In *The Internet Protocol Forum*, volume 14, 2011.
[3] NIST. NIST RPKI Monitor. https://rpki-monitor.antd.nist.gov/, 2025.
[4] Tomas Hlavacek, Haya Shulman, Niklas Vogel, and Michael Waidner. Keep your friends close, but your routeservers closer: Insights into RPKI validation in the internet. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 4841–4858, Anaheim, CA, August 2023. USENIX Association.
[5] Federal Communication Commission. FCC FACT SHEET * Reporting on Border Gateway Protocol Risk Mitigation Progress. https://docs.fcc.gov/public/attachments/DOC-402609A1.pdf/, 2024.
[6] The White House. Press Release: White House Office of the National Cyber Director Releases Roadmap to Enhance Internet Routing Security. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf, 2024.
[7] Koen van Hove, Jeroen van der Ham-de Vos, and Roland van Rijswijk-Deij. Rpkiller: threat analysis of the bgp resource public key infrastructure. *Digital Threats: Research and Practice*, 4(4):1–24, 2023.
[8] Donika Mirdita, Haya Schulmann, Niklas Vogel, and Michael Waidner. The cure to vulnerabilities in rpki validation. *NDSS Symposium*, 2024.
[9] Donika Mirdita, Haya Schulmann, and Michael Waidner. {SoK}: An introspective analysis of {RPKI} security. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 3649–3665, 2025.
[10] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Shulman. Are we there yet? on rpki's deployment and security. *Cryptology ePrint Archive*, 2016.
[11] Weitong Li, Zhexiao Lin, Md Ishtiaq Ashiq, Emile Aben, Romain Fontugne, Amreesh Phokeer, and Taejoong Chung. Rovista: Measuring and analyzing the route origin validation (rov) in rpki. In *Proceedings of the 2023 ACM on Internet Measurement Conference*, pages 73–88, 2023.
[12] John Kristoff, Randy Bush, Chris Kanich, George Michaelson, Amreesh Phokeer, Thomas C Schmidt, and Matthias Wählisch. On measuring rpki relying parties. In *Proceedings of the ACM Internet Measurement Conference*, pages 484–491, 2020.
[13] Khwaja Zubair Sediqi, Romain Fontugne, Amreesh Phokeer, Massimiliano Stucchi, Massimo Candela, and Anja Feldmann. Rpki syncing: Delay in relying party synchronization. 2025.
[14] RIPE NCC. RIS BGP Collectors. https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/archive/ris-raw-data, 2025.
[15] RIPE NCC. Ripestat. https://stat.ripe.net/, 2025.