Poster: Diverging Branches - How different are RPKI Trees across RIRs?

Deepak Gouda
deepakgouda@gatech.edu
Georgia Institute of Technology
Atlanta, USA

Cecilia Testart
ctestart@gatech.edu
Georgia Institute of Technology
Atlanta, USA

ACM Reference Format:
Deepak Gouda and Cecilia Testart. 2024. Poster: Diverging Branches - How different are RPKI Trees across RIRs?. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3646547.3689681

1 Introduction

Resource Public Key Infrastructure (RPKI) is a critical component in securing the inter-domain routing infrastructure today. More than 50% of the routed IPv4 and IPv6 prefixes are covered by RPKI Route Origin Authorizations (ROAs). ROAs are cryptographically verifiable records of the Autonomous System (AS) authorized to originate routes to a set of prefixes. Network operators are increasingly relying on RPKI to validate routing information and reduce the spread of BGP hijacks and misconfigurations. RPKI infrastructure has five root authorities maintained by the five Regional Internet Registries (RIRs). Each root authority independently implements its RPKI infrastructure, choosing how to manage certificate production from its self-signed root of trust certificate. In this poster, we study the different designs of RPKI infrastructure across the five roots and how these differences impact the characteristics of the RPKI Certificate repository, such as scalability and compute requirements. We discover that some RPKI repositories are computationally more expensive than others due to their design.

2 Dataset

To explore RPKI certificate repositories, we use raw RPKI certificates from the RIPE FTP repository [4], which collects all certificates from the five RIRs. We use `rpki-client`[1] to parse the individual certificates. We use the RPKI data of August 1, 2024 for this study. RPKI certificates follow the X.509 [2] format specification and contain crucial information such as the list of resources *i.e.,* the set of ASNs and IP prefixes associated with the certificate holder, certificate validity period, certificate issuer and the signature path used to sign the certificate. The RPKI certificates are hosted by five Root Certification Authorities (CA) and 88 delegated Certification Authorities - organizations authorized by the Root CAs to host and maintain their own RPKI repository.

3 Structural differences between RPKI Trees

The RIRs follow different practices while issuing RPKI certificates. At the top of the certificate hierarchy, each root authority hosts an offline certificate and uses it to issue a self-signed root certificate. The root certificate can issue downstream certificates for any IP address or Autonomous System Number (ASN). The root certificate signs multiple Resource Certificates (RCs), and assigns a subset of its pool of resources to each Resource Certificate.

Resource Certificates are cryptographically verifiable proof of the certificate holder's right to issue downstream certificates for its own pool of resources. We refer to RCs signed by a root certificate as RC-L1 and RCs signed by an RC-L1 certificate as RC-L2. In general, RC-L$[i]$ certificates are issued using RC-L$[i-1]$ certificates.

The five root certificates' resource pool spans the entire resource space *i.e.,* IPv4 space, IPv6 space, and all ASNs. RC-L1s of all RIRs except AFRINIC inherit the resource pool from their root certificate, mainly as an extra layer of security. ARIN goes one step ahead by issuing 11 RC-L2s, which again inherit the entire resource pool from RC-L1s. The other RIRs split their resource pool among the RC-L2s. The resource list among the RC-L2s is mutually exclusive, thus specifying which certificate can issue ROAs for which resource. In ARIN, the segregation of the resource list happens among the RC-L3 certificates. Accordingly, the issuance of ROAs happens at different levels for each RIR, which results in some ROAs having a longer chain of signatures than the rest. Fig 1 gives a more detailed outline of the RPKI tree structure among the five RIRs.

Each RC is associated with a Certificate Revocation List (CRL), a Manifest file (MFT), and a repository of ROAs (or additional certificates) signed using the RC. The MFT file contains the list of certificate objects that should be present in the current repository and the corresponding file hashes. RPKI validator software validates the integrity of the MFT file and then uses it to identify any missing or stale records [3]. The software then validates the files listed in the MFT. We refer to the combined set of MFT files in the entire RPKI repository as the MFT of the repository for brevity. The size of MFT varies significantly across the RIRs (Tab 1) due to their certification practices. We discuss the reason of this variance and its operational impact in the next section.

RPKI validator software validates the ROAs to extract Validated ROA Payloads (VRPs). VRPs are prefix-ASN pairs that indicate the ASN that is authorized to originate the prefix on BGP. A single ROA can contain multiple VRPs. RIRs choose to issue different number of VRPs in each ROA. RIPE aggregates several VRPs into a single ROA. In contrast, ARIN ROAs mostly contain one VRP. Thus, to issue the same number of VRPs, ARIN needs to create more ROA files than RIPE, which leads to operational differences discussed in the next section.

IMC '24, November 4–6, 2024, Madrid, Spain
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689681

	AFRINIC	APNIC	ARIN	LACNIC	RIPE
# ROA files	61973	68005	300112	57612	94059
μ(ROA size*)	1937	1908	2118	1953	1873
# files in MFT	9542	118805	165233	40650	90242
# certs in CRL	6252	112478	88099	28341	97199
# VRPs	7678	30308	145536	27674	45638
# RCs	780	8739	4564	5332	16138
μ(ROA/RC)	9.84	3.47	31.89	5.19	2.83
μ(VRP/ROA)	1.34	4.37	1.14	1.26	5.72
# BGP pfxes	19369	170155	119124	113186	242236

Table 1: Key metrics of RPKI repositories of five root authorities; μ refers to mean; *ROA file size is in bytes

4 Operational Implications

The structural differences in RPKI tree dictate several key characteristics of the certificates. Key attributes which impact the usage of a repository include the length of signature chain used to issue certificates and the number of certificate objects in the repository. In this section, we discuss how these attributes impact the RPKI repository's operations.

Length of signature chains : As discussed in Sec 3, RCs of different levels issue ROAs in each RIR. ARIN has 11 RC-L2s and distributes the workload of issuing ROAs equally among these certificates. In contrast, RIPE uses a single RC-L2 to sign 20.6K RC-L3s directly. LACNIC uses one RC-L2 to sign all RCs for NIC.br, the Brazilian National Internet Repository (NIR) and a second RC-L2 to sign RCs for all other LACNIC resources. The difference in structure of the certificates leads to a longer chain of signatures in some RIRs and shorter chains in others.

Validating a certificate requires performing cryptographic computations to check the entire signature chain used to issue the certificate. A longer chain of signatures requires more computations to assert the validity of the certificate since all the links from root certificate to the child have to be verified. Studying the number of signature links from root certificate to the ROAs in each RIR, we observe that APNIC and LACNIC certificates have the longest signature path lengths. Thus, ROAs in these repositories need more cryptographic computations per certificate than other repositories. In contrast, AFRINIC has the shortest signature path length on average and needs the least number of computations per certificate.

Number of files in RPKI repository : As mentioned in the previous section, RPKI validator softwares running in RPKI-deployed networks over the Internet download the RPKI repositories from all root authorities (and delegated CAs) periodically. Due to the design choices of RIRs, some RPKI repositories have more number of files than others. The validator downloads and validates each file in the repository. Thus, the higher number of files in certain repositories demand more computational operations than others.

The ARIN repository's MFT consists of 165K files (CRL and ROAs) which need to be validated, the highest across all RIRs. Each ARIN ROA contains 1.1 VRPs on average, which indicates that ARIN issues a new ROA for almost every VRP. In contrast, a RIPE ROA consists of 5.7 VRPs and an APNIC ROA contains 4.4 VRPs. Thus, to issue the same number of VRPs, ARIN would require 3.8*x*-5*x* the number for ROAs in APNIC and RIPE respectively. While APNIC and RIPE aggregate multiple VRPs into a single certificate, the practice of ARIN to issue a high number of individual ROA files leads to a large MFT file. Besides, the ARIN ROA files also have the highest average file size (Tab 1). Thus, in terms of repository size and the number of files to be processed, ARIN repository requires the highest amount of computation during validation.

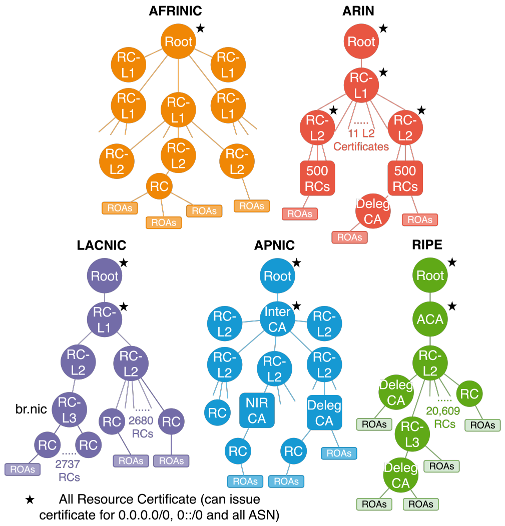

Figure 1: RPKI Structure of the five RIRs

Delegated CAs : Only RIPE, APNIC and ARIN have delegated CAs *i.e.,* RPKI infrastructure hosted by independent organizations. The RIPE repository consists of 44 delegated CAs. The APNIC repository contains 24 delegated CAs including the National Internet Registries (NIR) - JPNIC, IDNIC, TWNIC and CNNIC. The ARIN repository contains 21 delegated CAs with Amazon issuing the highest number of certificates for their own resources. All ROAs covering the prefixes delegated by AFRINIC are signed and hosted by AFRINIC.

The use of delegated Certificate Authorities may lead to operational discrepancies. Since the RPKI validator softwares fetch data from all repositories before starting the validation, if one repository faces a downtime, the validation procedure might face delays. The availability of Delegated CAs in APNIC, ARIN and RIPE gives more flexibility to their customers who want to maintain their own repository but also leads to potential operational disruptions.

Acknowledgements

This work is supported by the National Science Foundation grant OAC-2419735. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] Kristaps Dzonsons; Claudio Jeker; Job Snijders; Theo de Raadt; Sebastian Benoit; and Theo Buehler. 2024. rpki-client. Retrieved Aug 29, 2024 from https://rpki-client.org

[2] Dr. Warwick S. Ford, Dr. Santosh Chokhani, Stephen S. Wu, Randy V. Sabett, and Charles (Chas) R. Merrill. 2003. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647. https://doi.org/10.17487/RFC3647

[3] Oleg Muravskiy and Tim Bruijnzeels. 2018. RIPE NCC's Implementation of Resource Public Key Infrastructure (RPKI) Certificate Tree Validation. RFC 8488. https://doi.org/10.17487/RFC8488

[4] RIPE. 2024. RIPE FTP Server. Retrieved Aug 29, 2024 from https://ftp.ripe.net/ripe/rpki/