RPKI Service Risk Analysis
9 April 2019

John Curran, President and CEO

Purpose of the Brief

- Provide an overview of ARIN's RPKI services
- Summarize the potential for inadvertent service provider routing dependency on ARIN's RPKI services
- Review ARIN's ongoing analysis of risk issues related to offering RPKI services
- Outline potential strategies for risk mitigation being reviewed by ARIN

ARIN RPKI Service

- RPKI is an optional service that allows resource holders to declare which networks (autonomous systems) are authorized to route their address blocks
- Customers can create Route Origin Authorizations (ROAs) specifying the autonomous systems (AS#s) that are authorized to route a given address block and the resulting ROAs are securely published globally via ARIN's RPKI certificate authority
- Networks validating routes via RPKI confirm (for any address blocks with published ROAs) that any routes received for those address blocks specify the authorized AS#'s and discard routes for address blocks with ROAs but whose AS#'s don't match

ARIN RPKI Service (cont.)

- The IETF's operational guidelines for RPKI route origin validation[1] (ROV) specify that routes received for networks that have no matching ROA should continue to be treated as they are today; i.e. such routes should be utilized for routing decisions
- Thus RPKI protects customers with published ROAs from having ROV-networks listen to unauthorized routing of their address blocks, but does not have any effect on those which do not publish ROAs
- Similarly, route origin validation should not result in any direct routing impact at times when ARIN's RPKI CA is not available to publish customer ROAs – it is as if ARIN customers are no longer RPKI participants

ARIN RPKI Service – Relying Parties

- Those who utilize ARIN's RPKI CA information are referred to as ARIN RPKI "Relying Parties" – these are generally networks that utilize the ROAs and related information in the ARIN RPKI CA repository to conduct RPKI route origin validation
- ARIN's only control over utilization of its RPKI CA repository is via our agreements, and ARIN provides access to RPKI CA information via a cryptographic key (the "Trust Anchor Locator", or TAL) which is obtained via the ARIN webpage and obligates agreement to ARIN's Relying Party Agreement (RPA)
- This approach to distribute the ARIN TAL is unique to ARIN among the 5 RIRs, but ensures a legally binding agreement with RPKI relying parties

Impact of Theoretical RPKI Service Outage & Relying Party Issue

- Despite robust engineering, it is prudent to be prepared for the potential fallout of a significant outage of ARIN's RPKI service[2] – e.g. an outage which prevents publication of all ARIN customer ROA's for a period of 4 to 12 hours in duration
- As previously noted, such an outage should not have any adverse impact, since best practices require that relying parties conduct route validation in a manner that falls back to present routing practices when no ROA's can be obtained for a given address block
- But this presumes optimal configuration of a new and highly technical capability by all relying parties

Impact of ARIN RPKI Outage

- While RPKI adoption is modest today, the long-term intent is for RPKI to be robustly deployed by network operators globally
- Given widespread global RPKI adoption, it is likely that RPKI route validation would be in use by upwards of eight thousand networks globally[3]
- Once globally adopted, a prolonged ARIN RPKI outage would leave the vast majority of networks in ARIN's service region more susceptible to potential route hijacking (i.e. just as it is today)

Impact of an ARIN RPKI Outage (cont.)

- More importantly, during a prolonged ARIN RPKI outage, any networks globally that are not correctly configured (to properly fall back to unvalidated routing) would not be able to validate ARIN-region network routes, and their customers would temporarily lose connectivity to the majority of the Internet in the ARIN-region
- While any network adversely impacted by a significant outage would be themselves responsible due to their misconfiguration and thus improper reliance of the RPKI CA services, it risks litigation may occur

Impact of an ARIN RPKI Outage (cont.)

- Given past ratios of misconfiguration of Internet distributed technologies, it is reasonable to presume that a small percentage (e.g. 2%) of relying parties will have an inadvertent dependency on ARIN RPKI services, which would imply more than 100 networks globally (and their customers) are likely to lose access to much of the ARIN-region Internet for the duration of a prolonged ARIN RPKI CA outage
- There could also be significant adverse publicity associated with any such outage, and a party who claimed to be harmed might choose to seek damages from ARIN, despite a proximate cause being misconfiguration of route original validation by one or more relying parties

RPKI Risk Mitigation Approaches – ARIN Customers

- For ARIN customers utilizing RPKI services, risk mitigation is fairly straightforward due to their use of the services under the RPKI Terms of Service <https://www.arin.net/resources/rpki/tos.pdf> which provides for disclaimer of warranty, limitation of liability, and indemnification of ARIN against damages
- All ARIN RPKI customers also have an ARIN RSA which provides similar terms and conditions that are applicable by reference for "Services" provided to those customers
- The RSA contains indemnification language that helps to protect ARIN; note that ARIN does not charge specific fees for RPKI services

RPKI Risk Mitigation Approaches – Relying Parties

- For Relying Parties utilizing RPKI services, ARIN risk mitigation is based upon the browserwrap acceptance to the ARIN Relying Party Agreement that occurs when obtaining ARIN's TAL – this provides access to ARIN's RPKI repository under similar terms as the RPKI Terms of Services agreement
- The browserwrap acceptance and RPA terms are criticized by some in the community. The ARIN Board has directed a review occur of ARIN's RPKI risk mitigation strategy for Relying Parties[4]
- The potential amelioration of the existing RPA-based risk mitigation mechanism requires that the final recommendation consider the combination of approaches that best meets the risk mitigation requirements and community desire to have RPKI broadly available

Some Potential Relying Parties - Potential RPKI Risk Strategies

1. ARIN will continue to rely on existing RSA terms for ARIN-region Relying Parties
2. ARIN can seek additional insurance coverage for ARIN's defense regarding RPKI service claims as community reliance on RPKI grows.
3. Conducting RPKI Services Operational Failure Testing may also be considered
4. Suggestions to establish a Separate RPKI Services Affiliate

1. Reliance on existing RSA terms for ARIN-region Relying Parties

- ARIN likely will continue to need to rely on RSA indemnification via the existing RSA terms and conditions

2. Obtaining additional specific insurance for defense against RPKI service claims

- Given that the risk is predominantly with regard to litigation-related legal fees, *ARIN will explore obtaining additional insurance to cover legal costs associated with defending against such claims*
- Such additional insurance coverage may be unavailable
- There is an interaction between the insurability and the other elements of ARIN's RPKI risk – for example, it may be possible to obtain reasonable additional insurance coverage when there is a clearly binding RPA, but not otherwise.

3. Conducting RPKI Services Operational Failure Testing

- One potential strategy for ensuring that an operational outage does not cause undo impact to relying parties (those who do not properly configure their fallback) would be to periodically "fail" ARIN's RPKI CA service so network operators may better understand this potential scenario. But we will have to examine potential negative side effects before committing to this.

Possible Risk Strategy Outcomes

A. ARIN is being urged to revise its RPA with a reduced indemnification clause scope

- We will examine if thru some combination of reliance on the existing RSA, more insurance, and/or operational failure testing could permit ARIN to more tightly define the scope of the Relying Party Agreement indemnification clause
- This does not address the concern of ARIN currently requiring a browserwrap RPA agreement, and implications for those who wish to develop and distribute software which accesses ARIN's RPKI repository without any explicit acceptance of ARIN RPKI terms by the user

Possible Risk Strategy Outcomes

B. A revised RPA?

- ARIN has been urged to drop the RPA indemnification clause and rely instead on the disclaimer and limitation of liability
- This would significantly increase ARIN's risk profile while not addressing the desire of routing software developers to have access to the ARIN RPKI repository absent browserwrap acceptance of ARIN's RPKI terms

Possible Risk Strategy Outcomes

C. ARIN has been urged to provide access to the ARIN Repository without any RPA

- This would materially increase ARIN's legal risk profile.

Discussion?

Some notes & additional resources:

1. *"Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI)"*, Internet Engineering Task Force, Best Current Practice 185, https://tools.ietf.org/rfc/rfc7115.txt
2. *Despite robust engineering, both RIPE and ARIN RPKI CA services have suffered a prolonged outage since rollout (ARIN on 24 Oct 2018 & RIPE on 3 Feb 2013)*
3. *Based on approximately 8700 Transit ASes present in the Internet Routing Table, Weekly APNIC Routing Table Analysis,* http://thyme.rand.apnic.net