CTIC
Center for Technology, Innovation and Competition

Penn Law

An Update on Legal Barriers to RPKI Adoption

David A. Wishnick
Research with Christopher S. Yoo
University of Pennsylvania

June 12, 2019

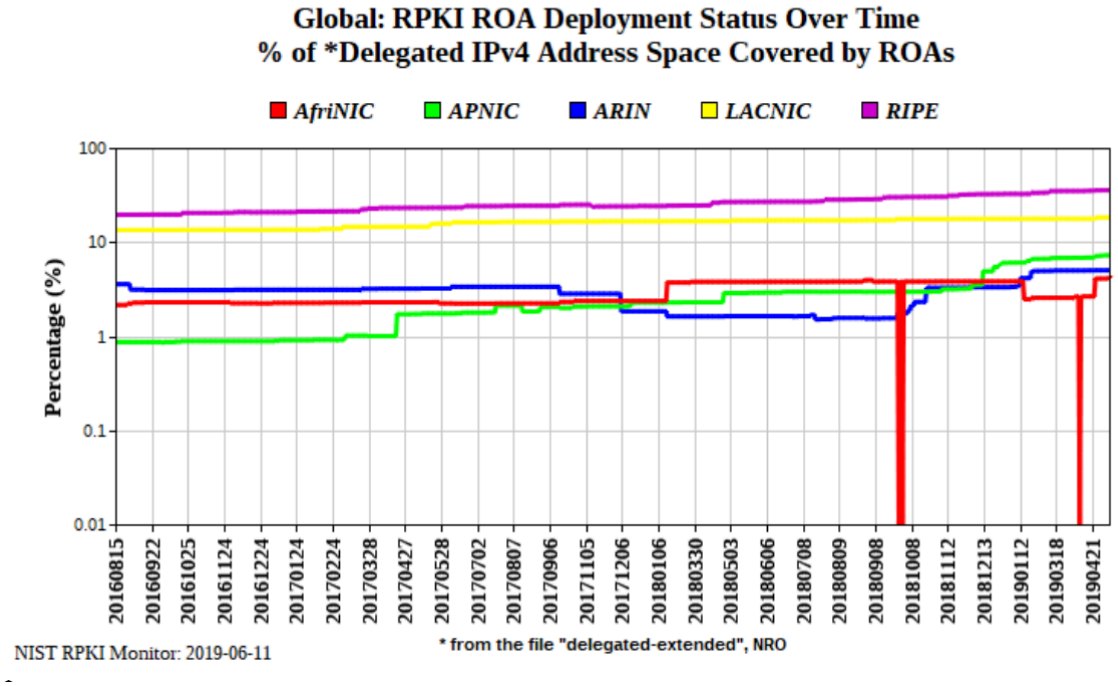
Research supported by NSF EAGER Award #1748362

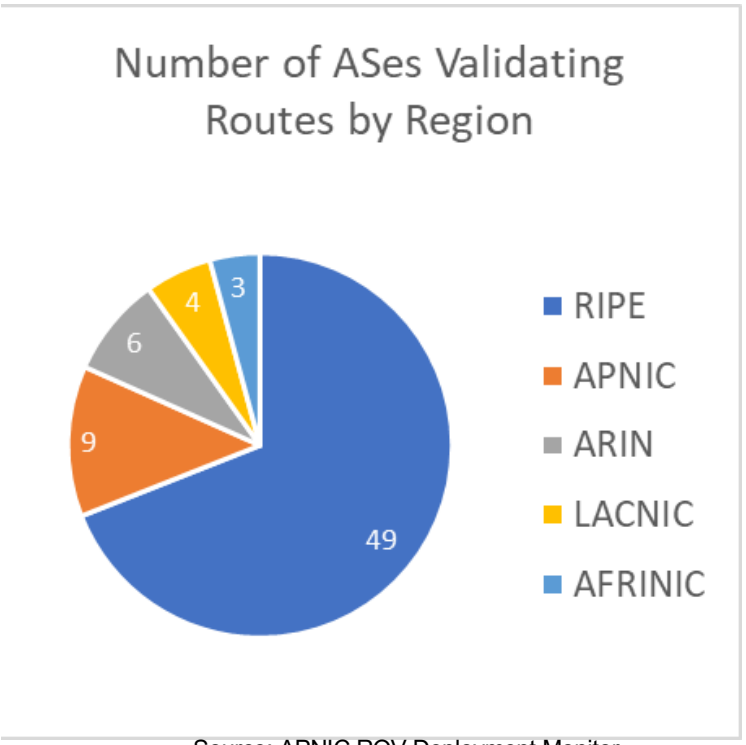
Intro to Resource Public Key Infrastructure (RPKI)

- RPKI protects against route hijacks by authenticating route origins
  - IP address holders create certificates identifying authentic IP address origins
  - Operators use validator software to verify that routes are pointing to correct origins
- Last 12 months have been eventful for RPKI
  - NTT began combining RPKI information with IRR data in July 2018
  - Amazon DNS was hijacked in Aug. 2018
  - Cloudflare committed to RPKI and began developing own validator software
  - AT&T began filtering routes (dropping invalids) in Feb. 2019
  - Google began flagging routes and will begin filtering routes in 2019
  - 100+ networks joined ISOC's Mutually Agreed Norms for Routing Security

Global RPKI Deployment

% of Declared IPv4 Space Covered By ROAs





Source: APNIC ROV Deployment Monitor

- 80% of those engaging in ROV omit the ARIN TAL (Cartwright-Cox, 2018)

NSF Grant on Legal Barriers to RPKI Adoption

- Motivation: reports that legal issues were slowing RPKI adoption in the ARIN region (particularly the RPA's indemnification clause)

- Methodology
  - Analysis of relevant contracts and policies
  - Interviews with broad range of stakeholders
  - Engagement with the ARIN and NANOG communities

Milestones

- Presentations at NANOGs 73-75
- Release of report and recommendations (Dec. 2018)
  - (Report link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3308619)
- Presentation at ARIN 43 (Apr. 2019)
  - ARIN has committed to conducting a full review, likely concluding by the end of 2019
  - Commenters encouraged swift action
  - One commenter even said, 'Increase our fees if it helps!'

Key Issues

- RPA acceptance/RPA clauses regarding liability
  - Elimination of the RPA vs. possible replacement of indemnification clause with as-is disclaimer
  - Possible creation of new nonprofit for RPKI
  - Integration of RPA acceptance into validator software

RPA Acceptance Through Routinator 0.4.0

```
Before we can install the ARIN TAL, you must have read
and agree to the ARIN Relying Party Agreement. It is
available at

https://www.arin.net/resources/manage/rpki/rpa.pdf

If you agree to the agreement, please run the command
again with the --accept-arin-rpa option.
Mascarpone:~ alex$ routinator init --accept-arin-rpa
Created local repository directory /Users/alex/.rpki-cache/repository
Installed the five TALs in /Users/alex/.rpki-cache/tals
Mascarpone:~ alex$ routinator -v vrps
rsyncing from rsync://rpki.ripe.net/ta/.
rsyncing from rsync://repository.lacnic.net/rpki/.
rsyncing from rsync://rpki.apnic.net/repository/.
rsyncing from rsync://rpki.afrinic.net/repository/.
rsync://rpki.ripe.net/ta: The RIPE NCC Certification Repository is subject to Terms and Conditions
rsync://rpki.ripe.net/ta: See http://www.ripe.net/lir-services/ncc/legal/certification/repository-tc
rsync://rpki.ripe.net/ta:
Found valid trust anchor rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer. Processing.
rsyncing from rsync://rpki.ripe.net/repository/.
Found valid trust anchor rsync://rpki.afrinic.net/repository/AfriNIC.cer. Processing.
rsyncing from rsync://rpki.arin.net/repository/.
Found valid trust anchor rsync://rpki.arin.net/repository/arin-rpki-ta.cer. Processing.
```

Key Issues

- RPA acceptance/RPA clauses regarding liability
  - Elimination of the RPA vs. possible replacement of indemnification clause with as-is disclaimer
  - Integration of RPA acceptance into validator software
  - Possible creation of new nonprofit for RPKI
- Revisions to the RPA's prohibited conduct clause
- Inclusion of RPKI in procurement requirements
- Information regarding best practices
- Other recommendations

Deployment of Best Practices

- RPKI deployment is only valuable if done safely (esp. failover)
- For network operators, best practices exist
  - Operators should follow the advice of the key RFC 7115 and 6480
  - Operators should solicit advice—from MANRS, Internet2, RIRs
- For RIRs, best practices require disclosure around service levels and perhaps increased service commitments

Potential Next Steps

- ARIN should consider RPA changes
  - Revising the liability provisions or dropping the RPA
  - Enabling machine-readable redistribution of RPKI info
- The ARIN community should consider whether to support the development of a new nonprofit for RPKI certificate publication
- Network operators and RIRs should focus on best practices and high-leverage tactics like requiring RPKI from vendors
- Everyone interested in enhancing routing security should keep up the momentum

Questions and Discussion