CTIC
Center for Technology, Innovation and Competition

Penn Law

Legal Barriers to Securing the Routing Architecture

Christopher S. Yoo
David A. Wishnick
University of Pennsylvania Law School

October 1, 2018

Research supported by NSF EAGER Award #1748362

This Study

- Origins
  - Perceived differences in Resource Public Key Infrastructure (RPKI) adoption in Europe and Latin America vs. North America
  - Concerns regarding potential legal barriers to RPKI adoption in North America
  - National Science Foundation's interest in translational research
- Goals
  - Catalog the claimed barriers to RPKI adoption
  - Independently evaluate the legal and institutional barriers
  - Suggest viable solutions that balance the interests of all stakeholders

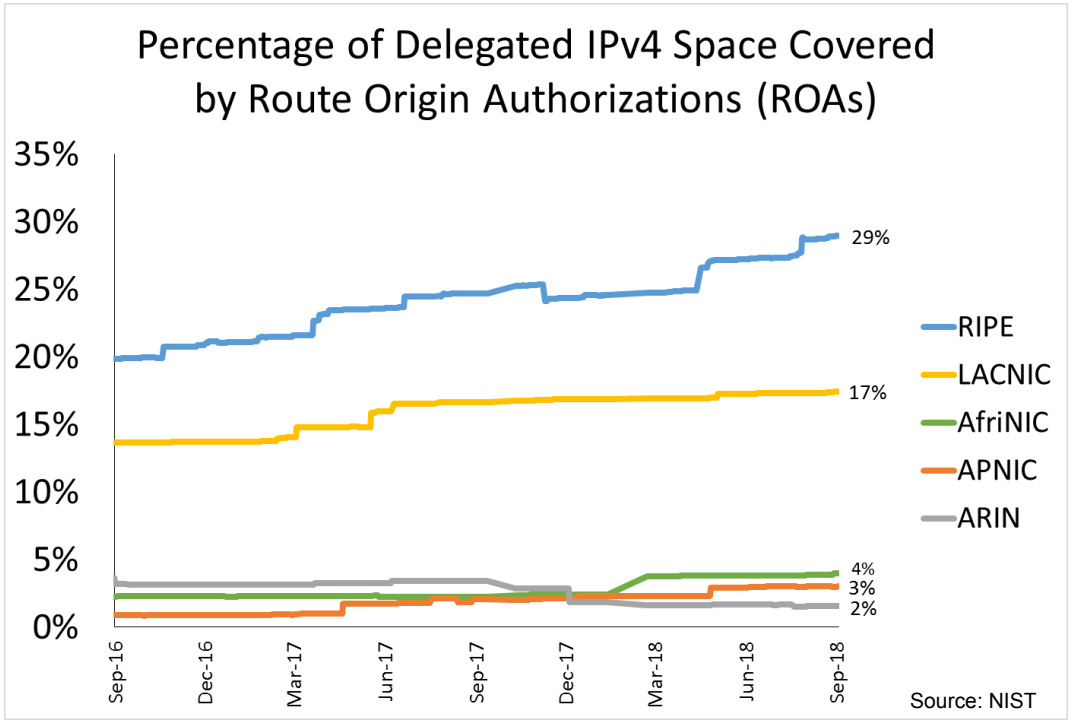
This Study

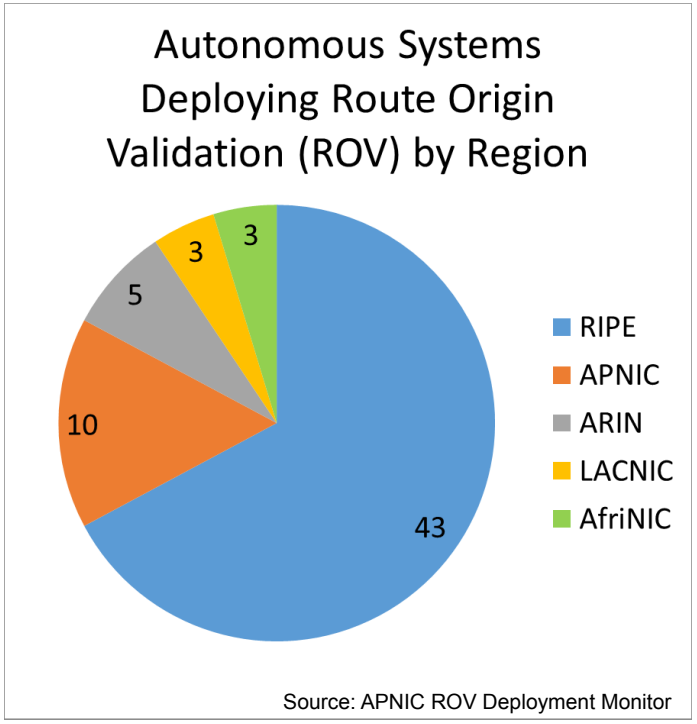
- Methods
  - Independent legal analysis
  - Interviews with over three dozen members of the routing community
    - Types of organizations include commercial firms, government, academia, and nonprofits
    - Roles include engineers, lawyers, researchers, and policymakers
  - Discussions with American Registry of Internet Numbers (ARIN) and other key stakeholders
- Focus
  - General evaluation of current regime
  - Comparison across different regions

Presentation Roadmap

- **Background**
- RPKI-based filtering
- RPKI-based signing
- Other legal mechanisms to spur deployment
- Potential next steps for the routing community

Global RPKI Deployment





- ARIN's repository appears less utilized than others (Cartwright-Cox, 2018)

Non-Legal Barriers

- Limited demand for RPKI and limited budgets
- Difficulty reaching critical mass
  - RPKI provides limited value until both signing and filtering are widespread
  - The ease of each depends on software and support
- Concerns about lack of robust software tools

Presentation Roadmap

- Background
- **RPKI-based filtering**
- RPKI-based signing
- Other legal mechanisms to spur deployment
- Potential next steps for the routing community

RPKI-Based Route Filtering

- Filtering entails dropping or "depreferring" routes based on RPKI information
- Requires access to RPKI certificate repositories offered by the Regional Internet Registries (RIRs)
  - Direct access: use of RPKI repositories (via Trust Anchor Locators, or TALs) to conduct Route-Origin Validation (ROV)
  - Indirect access: third-party provision of route-filtering support built atop ROV

Legal Structure of TAL Access

- Leading validator software provided by Réseaux IP Européens Network Coordination Centre (RIPE NCC) comes preloaded with all TALs except ARIN's

```
The Trust Anchor Locator (TAL) files for four Regional Internet Registries are included
with this distribution: AFRINIC, APNIC, LACNIC and RIPE NCC.

To access ARIN's TAL, you will have to agree to ARIN's Relying Party Agreement. Please
visit this ARIN web page for more information:

  https://www.arin.net/resources/rpki/tal.html
```

- Four RIRs allow access to TALs without agreements
- ARIN requires acceptance of a Relying Party Agreement (RPA)

Barriers to TAL Access

- Visiting ARIN's site is not a serious *technical* barrier
- But the RPA is an *institutional* barrier
  - Increased difficulty distributing validation software with ARIN's TAL preloaded (but may have made some progress)
  - Need for legal approval

Risks of TAL Provision

- All actors should reduce operational risk
  - Prepare for potential RPKI outages (e.g., RIPE NCC Feb. 2, 2013)
  - Prepare for conflicting data in multiple RPKI repositories (may be solved)
  - Configure operations to accommodate such contingencies (see RFC 7115)
- Community needs to assess legal risks amid uncertainty
  - There are no direct legal precedents
    - No record of lawsuits against an RIR for RPKI
    - No record of lawsuits against providers of the roots for TLS, SSL, DNSSEC, or IRR
  - But past history does not guarantee future results (i.e., lack of past lawsuits in other contexts does not guarantee no future lawsuits over RPKI)

Legal Risks of TAL Provision

- Low risk of strict products liability for RPKI
- Negligence liability is manageable, but cannot be eliminated
  - Industry best practices can establish reasonableness of RIRs' practices
  - User misuse is a defense
  - Tail risks still remain (especially in light of the litigiousness of the U.S.)
  - Negligence is often a jury question (cannot always end litigation early)
- Residual risk of defense costs justifies the existence of the RPA
  - Even rapidly dismissed cases require resources to defend
  - Contract terms represent the traditional way to manage such risks
  - U.S. law requires explicit agreement (online terms & conditions not sufficient)

Optimizing TAL Access

- Can we do more to enable possibilities for third-party providers?
  - We have already made some progress, thanks to a constructive dialog on the NANOG listserv
  - Community is now exploring ways to build click-through approval into distribution system for validator software
- Are there particular clauses that bear closer scrutiny?
  - Prohibited conduct clause
  - Indemnification, arbitration, and choice of law clauses

Prohibited Conduct Clause

- Prohibits sharing RPKI info in "machine-readable format"
- Blocks potentially valuable research and third-party software support
- Hinders integrated provision by third-party providers that combine RPKI information with other information (e.g., DNS, IRRs) to support real-time routing

RIR Prohibited Conduct

RIR	RPA Analogs: Prohibited Conduct (Paraphrases)
ARIN	Prohibits sharing in a machine-readable format
AFRINIC	No agreement
APNIC	No specific prohibitions
LACNIC	No agreement
RIPE NCC	Prohibits use for unsanctioned purposes, including advertising, market research, and similar

Proposal for Prohibited Conduct

- Discussions are ongoing whether to revise to permit reasonable, security-focused sharing and research (not for real-time routing)
- Community should consider the potential benefits of enabling sharing of machine-readable RPKI information to enable combining ROAs with other information to support real-time routing

Governmental TAL Access

- Some governmental entities can't sign indemnification, arbitration, or choice-of-law clauses
  - U.S. Antideficiency Act
  - California State Contracting Manual
- ARIN already alters the RPA for these entities
- ARIN and NANOG community should broadly publicize this policy
- Government agencies should share information about such alterations

Nongovernmental TAL Access

- Some claim indemnification clause poses a barrier
- Clause triggers organizational policies requiring legal consultation
- Clause raises risk
  - Note: organizations sign indemnification clauses in other contexts
  - Question is whether benefits of doing so exceed the risks

RIR Indemnification: Validation-Side

RIR	RPA Analogs: Key Clauses Allocating Liability (Paraphrases)
ARIN	• Disclaimer of warranties • Indemnify, defend, and hold harmless • Applies to claims asserted by third parties in connection with actions taken by the RP or users downstream of the RP
AFRINIC	• No agreement
APNIC	• No agreement; online terms and conditions include indemnification, but not duty to defend or hold harmless
LACNIC	• No agreement
RIPE NCC	• Disclaimer of warranties

Alternative Contractual Approaches to the RPA

- Indemnification clause
- "As is" disclaimer of warranties and statement of risks
  - Commonly seen in software and information licenses
  - Reduce risk of negligence liability
  - Also employed by RIPE NCC
  - May require more extended court proceedings to establish non-liability

Evaluating Exclusive Reliance on "As Is"

- Arguments in favor
  - Would bring ARIN in line with other RIRs
  - Would bring the RPA in line with agreements for DNS Root Trust Anchors, OpenSSL Toolkit
- Arguments against
  - Would be less protective to ARIN than other agreements (*i.e.*, ISP service agreements)
  - May impose greater costs on ARIN for benefits to the larger community

Presentation Roadmap

- Background
- RPKI-based filtering
- **RPKI-based signing**
- Other legal mechanisms to spur deployment
- Potential next steps for the routing community

RPKI Key Access by Government

- To access RPKI private keys, address space holders must sign a Registration Services Agreement (RSA) or a Legacy RSA (LRSA)
- RSA/LRSA clauses raise similar problems to RPA
  - Indemnification clause
  - Choice-of-law clause
- ARIN already offers a similar solution (alters the RSA and LRSA for these entities)
- ARIN and NANOG community should broadly publicize this policy
- Government agencies should share information about such alterations

RPKI Key Access by Legacy Address Holders

- LRSA contains a "no property rights" acknowledgment
  - Unclear whether this is a "but for" barrier to RPKI adoption—but still a barrier
  - Interesting data point: low levels of RPKI deployment in IPv6
- Issue of residual ownership is conceptually independent from RPKI key access
  - Our analysis does not mean to take a position on this issue
  - Our analysis attempts to decouple the two issues

RIPE NCC's Approach to Decoupling the Issue

- RIPE NCC offers a "non-member services" pathway
  - Provides access to RPKI keys
  - Does not require registration
  - Does not address issue of transfer rights
  - Is provided pursuant to conditions
  - Requires payment of a fee (€1,400 annually/same as membership fee)

Presentation Roadmap

- Background
- RPKI-based filtering
- RPKI-based signing
- **Other legal mechanisms to spur deployment**
- Potential next steps for the routing community

Procurement Policy

- Procurement policies can prompt suppliers to act
- The private sector has leverage
  - Major customers and network actors can push suppliers to implement RPKI (e.g., AMSIX)
  - Private actors can consider joining consortia like Mutually Agreed Norms for Routing Security (MANRS)
  - Major actors can include RPKI in compliance checklists
- The public sector has significant leverage as well
  - Governmental policy has pushed for the adoption of past security measures
  - NANOG community should consider whether to advocate for governmental RPKI requirements

Presentation Roadmap

- Background
- RPKI-based filtering
- RPKI-based signing
- Other legal mechanisms to spur deployment
- **Potential next steps for the routing community**

Next Steps

- Build on current progress
  - Potentially embedding approval of RPA in validator software distribution
  - Potential revisions to the prohibited conduct clause
  - Acknowledgement of exceptions for government entities
- Make sure the entire community understands the requirements for best-practices compliance
- Address the non-legal barriers to RPKI adoption
- Evaluate proposals to alter ARIN's RPKI-related agreements
- Evaluate including RPKI in procurement requests
- Engage in dialogue re community-level goals for routing security

Questions and Discussion