Legal Barriers to Securing the Routing Architecture

David A. Wishnick
Christopher S. Yoo, lead author
University of Pennsylvania Law School
October 15, 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
Global RPKI Deployment

ARIN’s repository appears less utilized than others (Cartwright-Cox, 2018)
Law and Routing Security

- Non-legal barriers are more significant than legal ones
  - Limited demand for RPKI
  - Limited budgets
  - Chicken-and-egg problem
  - BUT growing interest appears to be changing the balance

- Legal issues create institutional barriers
  - Legal agreements increase friction inside organizations
  - Legal controversy and uncertainty exacerbate the chicken-and-egg problem
Areas Where We Have Already Made Progress

- Remove indemnification, arbitration, and choice-of-law clauses for appropriate government entities
- Potentially embed click-through approval of RPA in validator software distributions
- Potentially revise the prohibited conduct clause to permit sharing of RPKI-derived information in a machine readable format
Legal Structure of TAL Access

- Leading validator software 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 Regional Internet Registries (RIRs) allow access to TALs without agreements
- ARIN requires acceptance of a Relying Party Agreement (RPA)
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, NANOG, and I2 communities 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
Potential Strategies to Improve TAL Access

- Keep ARIN’s RPA, but enable software implementations that require click-through acceptance of the RPA
- Keep ARIN’s RPA, but remove the indemnification clause
- Eliminate ARIN’s RPA
Three Ways to Form a Contract

- Click-through or clickwrap – requires explicit acceptance of terms and conditions
- Browsewrap – posts terms and conditions next to the button for downloading software and infers that download = acceptance
- Posting terms and conditions on a separate webpage

- Clickwrap and browsewrap are likely to form contracts
- Simply posting terms and conditions is unlikely to form contracts under U.S. law
Comparison to Other Resources

- Many resources are provided without RPAs
  - Comodo TLS/SSL root
  - DNSSEC root (IANA)
  - AfriNIC, LACNIC RPKI repositories
- Many resources are provided “as is” via browsewrap licenses
  - Geotrust TLS/SSL root
  - RIPE NCC RPKI repository
Evaluating Keeping/Eliminating the RPA

- **Primary arguments in favor of eliminating the RPA**
  - Would ensure the widest possible distribution of RPKI keys
  - Is not required by other resources, such as DNSSec

- **Primary arguments against eliminating the RPA**
  - Would eliminate “as is” disclaimer relied on in many other contexts
  - Would leave allocation of risk to ex post litigation

- **Ultimate choice depends on how the community would like to resolve the tradeoffs**
Evaluating Exclusive Reliance on “As Is”

Arguments in favor

- Would bring ARIN in line with other RIRs
- Would ensure reasonable risk-sharing
  - Depends on the community understanding best-practices compliance (RFC 7115)
  - Should be backed by clear disclosure in ARIN’s Certification Practice Statement
  - Example: adopt policies that do not automatically treat “unknown” as “invalid”

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
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

<table>
<thead>
<tr>
<th>RIR</th>
<th>RPA Analogs: Prohibited Conduct (Paraphrases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARIN</td>
<td>Prohibits sharing in a machine-readable format</td>
</tr>
<tr>
<td>AFRINIC</td>
<td>No agreement</td>
</tr>
<tr>
<td>APNIC</td>
<td>No specific prohibitions</td>
</tr>
<tr>
<td>LACNIC</td>
<td>No agreement</td>
</tr>
<tr>
<td>RIPE NCC</td>
<td>Prohibits use for unsanctioned purposes, including advertising, market research, and similar</td>
</tr>
</tbody>
</table>
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
Legacy Registration Services Agreement (LRSA)

- Debate the merits of decoupling residual ownership of the address space from RPKI by following RIPE NCC’s example of a non-member services agreement
- Depends on recognizing that creating a non-member services agreement would not implicitly validate either position
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, I2, and NANOG communities 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)
Next Steps

- Build on current progress
  - Embedding approval of RPA in validator software distribution
  - Potential revisions to the prohibited conduct clause
  - Acknowledgement of exceptions for government entities
- Evaluate proposals to alter ARIN’s RPKI-related agreements
- Evaluate including RPKI in procurement requests
- Address the non-legal barriers to RPKI adoption
- Engage in dialogue re community-level goals and best practices for routing security
Questions and Discussion