Overcoming Legal Barriers to RPKI Adoption

Christopher S. Yoo
University of Pennsylvania
December 10, 2019
Research supported by NSF EAGER Award #1748362
80% of those engaging in ROV omit the ARIN TAL (Cartwright-Cox, 2018)
Initial Observations

- Real-world developments
  - Filtering by AT&T/interest by Google and Cloudflare
  - New validator software by Cloudflare and NLnet Labs
  - Use of RPKI by NTT to clean up Internet Routing Registry (IRR)
  - Complications surrounding JPNIC’s deployment and outage by ARIN
  - ARIN revisions on October 21, 2019

- Legal concerns
  - Need for address holders to sign Registration Services Agreement (RSA)
  - Decision whether to maintain own ROAs or delegate to ARIN
  - Need for ISPs to accept Relying Party Agreement (RPA) on ARIN’s website
Existence of the Relying Party Agreement (RPA)

- **Current practice:** requirement of click-through acceptance of RPA to access ARIN’s TAL (unique to ARIN; others use online terms)

- **Our recommendation**
  - Acknowledge existence of valid arguments for abolishing and keeping RPA
  - Explore incorporation of acceptance into distribution of validator software
  - Explore enterprise-level agreements

- **ARIN’s decision**
  - Retain RPA because of litigiousness of U.S./overhanging negligence liability
  - Enable integration of RPA acceptance into validator software
  - Note: no cases on record re RPKI, TLS, SSL, DNSSec, or IRR
RPA Terms – Indemnification

- Current practice: requirement to indemnify, defend, hold harmless
  - RIPE NCC: online terms include disclaimers of warranties
  - APNIC: online terms include indemnification (no duty to defend)
  - LACNIC and AFRINIC: no clauses

- Our recommendation
  - Replace indemnification with as-is disclaimer/no consequential damages
  - Consider creating separate entity for RPKI to limit liability

- ARIN’s decision
  - No indemnification for gross negligence or willful misconduct
  - Inclusion of as-is disclaimer, no consequential damages, limitation of liability
RPA Terms – Prohibited Conduct Clause

- Current practice: prohibition of sharing RPKI-derived information in a “machine-readable format”
  - Blocks use for error reporting and research
  - Blocks real-time uses/integration into IRRs
  - Note: other RIRs have no analogous provision

- Our recommendation: revise to permit research and real-time uses

- ARIN’s decision
  - Allowance of use of RPKI-derived data for informational purposes
  - Creation of Redistributor RPA: can distribute info to third parties who signed RPA and passed through terms limiting liability and indemnification
RSA Terms

- Current practice
  - Willingness to waive indemnification and choice of law when required by law
  - Requirement that legacy holder acknowledge no property rights in addresses

- Our recommendation
  - Publicize willingness to waive clauses when required by law
  - Follow RIPE NCC’s creation of a non-member services agreement

- ARIN’s decision
  - No changes to terms (still includes blanket indemnification)
  - No publicity about willingness to waive

- Legacy holders sign RSAs for IPv6; RPKI not deploying for IPv6
Other Possible Developments

- Inclusion of RPKI in public and private procurement requirements
- Education about the proper configuration by ISPs (esp. failover)
- Broader disclosure of ARIN’s practices
  - Information on uptime, update frequency, response expectations, etc.
  - Expanded Certification Practice Statements
  - Clear guidance about best practices/incentive to deploy them
- More robust software tools (new Cloudflare & NLnet validators)