Legal Barriers to Securing the Routing Architecture

David A. Wishnick
University of Pennsylvania Law School
June 26, 2018
Research supported by NSF EAGER Award #1748362
Problem

- BGP updates to routing tables are unverified
- Unverified routes are vulnerable to mistakes/hijacks
  - Late ‘90s: AS 7007, 8584 announce routes to large pieces of the Internet
  - Late ‘00s: Yahoo! unreachable; YouTube diverted
  - Late ‘10s: Financial services traffic diverted; cryptocurrency stolen
A Partial Solution: RPKI

- A global initiative to validate BGP routing announcements
- *Origin* validation, not path validation
- Gives encryption keys to IP address holders
- Has address holders sign Route Origin Authorizations (ROAs) verifying that the last hop is pointing at the right address
- Enables network providers filter out unsigned routes (Route Origin Validation, or ROV)
Global RPKI Deployment

- Difficult to estimate ROV (Reuter et al., 2018)
Project Background

- NSF EAGER Grant

- Goals
  - Understand the barriers to RPKI adoption
  - Propose viable solutions to any legal barriers—solutions that respect all stakeholders
Why Might Regional Adoption Rates Differ?

- Economic incentives?
- Culture?
- Internet topology?
- Law?
Uncovering the Barriers

- Interviews across the routing community
  - Commercial firms
  - Academic institutions
  - Governmental entities
  - Engineers
  - Researchers

- Independent contractual analysis
  - RIR agreements
  - Agreements governing comparable services
Seeking Your Input

- Your experiences with RPKI and services like it
- Your organization’s approach to procurement
- Your views about the deployment path for RPKI

- Find me in the hall, or email me to set up a conversation: dwishn@law.upenn.edu

- Thank you!