Internet routing registries (IRRs), data governance and security

Brenden Kuerbis and Milton Mueller
School of Public Policy
Georgia Institute of Technology, United States
Introduction

Supply and use of route announcement and policy data is highly distributed and decentralized, permitting many opportunities for errors or manipulation.

Yet, distributed and decentralized exchanges of information among ISPs also makes the system flexible and responsive to local conditions.
The routing security problem

Not just a technical problem, but a governance of data problem.

- Organizational practices, contracts, policies, etc.

Exchange of data - BGP announcements and AS policy objects, Internet routing registries - is essential to accurate routing.

Differing, conflicting motivations of suppliers and users of data.
Existing form of routing data governance

...and why it is broken

**IRRs** - multiple, diverse organizations for sharing routing policy information (route objects, AS-sets, etc.)

- **Misaligned incentives**
  - Privacy of data
  - Collective action problem, under production of public good
  - Costs/benefits of data maintenance

- **High transaction costs**
  - RPSL difficult, not uniformly used
  - No systematic identification of authentic, accurate, or obsolete data
  - Limited benefits of mirroring data
  - Anomalies/filtering costs greater for some ASes

- **Unmanageable interdependencies**
  - Unilateral changes in data can have unexpected, undesired consequences
Existing data governance alternatives to improve routing security...have shortcomings

**RPKI and BGSPEC**

- *Ex ante* elimination of BGP announcement vulnerabilities
- Hierarchical, potential new risks (Cooper et al, 2013; Mueller & Kuerbis 2011)
- Real-time validation creates additional costs, requires some collective action too (Goldberg, 2014)
- Doesn’t address some routing vulnerabilities (Huston, 2015)
- Resource certification with routing policy data (Blunk, 2004; Karir & Blunk, 2011; Goldberg, 2014; Kisteleki & Haberman, 2016)

**Route monitoring services**

- *Ex post* mitigation of BGP announcement vulnerabilities
- Turns functionality of public, shared good (IRR) into private good
Data governance alternatives for routing security

Mutually Agreed Norms on Routing Security (MANRS)

- Operators should set, exchange, validate, enforce routing policies; validate resource authorization...
- Challenges of operator diversity, evolving practices, community enforcement, constraints

A blockchain Internet routing registry? (BIRR)

- Another way to do trusted attestations?
- Distributed database with transactions securely recorded to a permanent ledger
- Key characteristics - distributed consensus, provable timeline, unforgeable transactions
Does either one resolve the economic issues?
<table>
<thead>
<tr>
<th>Economic issue</th>
<th>Existing IRR system</th>
<th>MANRS</th>
<th>Blockchain IRR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Misaligned incentives</strong></td>
<td>No privacy of routing policies</td>
<td>Makes policies private to ASes exchanging data</td>
<td>Can make policies private under certain implementations; combine open and closed blockchains</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Collective action among all operators</td>
<td>Reduces collective action to any specific AS and its customer and adjacent ASes</td>
<td>Could emphasize collective action of routing registry operators; requires standardization of distributed consensus protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weak incentives to delete or update objects</strong></td>
<td></td>
<td></td>
<td>Objects never deleted from registry</td>
</tr>
<tr>
<td>Economic issue</td>
<td>Existing IRR system</td>
<td>MANRS</td>
<td>Blockchain IRR</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>High transaction costs</strong></td>
<td>RPSL inadequate, difficult to use</td>
<td></td>
<td>Digital signature over object using key data provides object authenticity, integrity; objects are sequential</td>
</tr>
<tr>
<td></td>
<td>No systematic way to validate authenticity or accuracy of objects; identify obsolete objects</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No data consistency across registries</td>
<td></td>
<td>Single, distributed registry</td>
</tr>
<tr>
<td></td>
<td>Filtering not scalable for large ISPs</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Unmanageable interdependencies</strong></td>
<td>Unilateral changes to route objects can have unanticipated consequences for other operators</td>
<td></td>
<td>Objects never deleted</td>
</tr>
</tbody>
</table>
Thanks. Feedback and questions?

brenden.kuerbis
milton.mueller
@pubpolicy.gatech.edu