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?

Do MANRS or blockchain address IRR data governance issues?

Economic issue	Existing IRR system	MANRS	Blockchain IRR
Misaligned incentives	No privacy of routing policies	Makes policies private to ASes exchanging data	Can make policies private under certain implementations; combine open and closed blockchains
	Collective action among all operators	Reduces collective action to any specific AS and its customer and adjacent ASes	Could emphasize collective action of routing registry operators; requires standardization of distributed consensus protocol
	Weak incentives to delete or update objects		Objects never deleted from registry

Economic issue	Existing IRR system	MANRS	Blockchain IRR
High transaction costs	RPSL inadequate, difficult to use		
	No systematic way to validate authenticity or accuracy of objects; identify obsolete objects		Digital signature over object using key data provides object authenticity, integrity; objects are sequential
	No data consistency across registries		Single, distributed registry
	Filtering not scalable for large ISPs		
Unmanageable interdependencies	Unilateral changes to route objects can have unanticipated consequences for other operators		Objects never deleted

Thanks. Feedback and questions?

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