Internet routing registries, data governance, and security

Brenden Kuerbis & Milton Mueller

To cite this article: Brenden Kuerbis & Milton Mueller (2017): Internet routing registries, data governance, and security, Journal of Cyber Policy, DOI: 10.1080/23738871.2017.1295092

To link to this article: http://dx.doi.org/10.1080/23738871.2017.1295092

Published online: 13 Mar 2017.
ABSTRACT
Routing is fundamental to the workings of the internet, yet the basic routing protocol, Border Gateway Protocol (BGP), is known to be insecure. This paper uses institutional economics to examine internet routing registries, which are used by network operators to mitigate the security flaws in BGP. Secure routing of internet traffic is characterised as a problem in the distributed governance of data. The highly distributed and decentralised exchange of routing announcements and routing policy data among network operators affords many opportunities for error or manipulation. This paper considers various solutions to the data governance problems associated with routing, in light of actors’ incentives and collective action problems. We compare IRRs to other methods of governing routing data in a way that enhances internet security, such as Resource Public Key Infrastructure and Border Gateway Protocol Security, Mutually Agreed Norms on Routing Security, and a blockchain supported routing registry.

1. Introduction
A typical internet-connected laptop or home computer can easily send 1 million packets of data per day, and receive 4–5 million a day. As a packet-switched network, the internet must transport every one of these data packets across the network individually. How do all of these packets know how to find their way from their origin to their destination, automatically and rapidly, and on such a massive scale? The answer is provided by the Border Gateway Protocol (BGP), a standardised method of exchanging information that internet service providers (ISPs) use to guide packets of data from their source to a destination. This process is known more generally as inter-domain routing, or simply routing. Routing relies on intensive and rapid exchanges of internet Protocol (IP) address prefixes and autonomous system numbers (ASNs) amongst network operators that advertise their ability to handle packets destined for specific IP address ranges.

Routing is fundamental to how the internet works. But while trillions of packets flow across the network as intended every hour, the internet’s BGP protocol is known to be susceptible to errors and attacks. Occasionally routing incidents or failures occur that knock major websites off the internet entirely, or divert large quantities of traffic (see, e.g. Cowie 2010; RIPE NCC 2008). Some of these problems occur because of the intentional publication of false information about origin IP addresses, others occur because of...
mistakes. As such, there are longstanding efforts to make routing protocols more secure, and to improve operational practices to avoid these problems.

This paper will examine routing security as a problem in the distributed governance of data. It will consider various solutions to the data governance problems associated with routing, including internet routing registries (IRRs), Resource Public Key Infrastructure (RPKI), Border Gateway Protocol Security (BGPSEC), Mutually Agreed Norms on Routing Security (MANRS), and blockchain technology.

We will show how the insecurity of BGP stems from the way routing data is exchanged among ISPs. The supply of routing announcements and routing policy data is highly distributed and decentralised. This creates many opportunities for error or manipulation. At the same time, however, distributed and decentralised exchanges of information among ISPs also give the network operators a great deal of autonomy, which makes the system freer, more flexible, and responsive to local conditions. With its IRRs, the internet community has developed a decentralised set of networked governance mechanisms for handling routing policy data. In theory and intent, these data can be used by ISPs to validate and filter routing announcements exchanged between networks using the BGP. As such, IRRs are currently one of the most important governance structures for BGP routing.

This paper is the first to examine IRRs from the standpoint of the economics of information security. It will document the supply of IRRs and what is known about their usage, while exploring the various governance structures they use to control the entry, updating, accuracy, and usage of routing policy data. This analysis, in combination with prior empirical work, will provide a more accurate and theoretically grounded view of the security shortfalls of IRRs.

In the debates over routing security, the inadequacies of IRRs are often targeted. Most of the proposed alternatives to IRRs, however, would make the governance of routing data more centralised and hierarchical. From a purely technical standpoint, hierarchy can make it easier to impose control over, and derive authority from, a complex and diverse system. However, hierarchical governance structures can also create new problems of their own – without necessarily eliminating the possibility of some common types of routing anomalies (Cooper et al. 2013; Kuerbis and Mueller 2011). The paper compares IRRs to proposed new forms of routing data governance, especially those based on proposed IETF standards such as RPKI and BGPSEC. The paper examines how RPKI might be used in conjunction with IRRs to overcome some of their known problems. The paper will conclude by briefly considering a normative effort to improve routing security, known as MANRS, and also consider blockchain as an alternative method of governing routing policy data in a way that enhances routing security.

2. The routing security problem

Routing security is a governance problem, not just a technical problem. Organisational and institutional factors – known as governance structures in institutional economics (Palay 1984; Williamson 1985, 1996) – are as important to internet routing security as technological design. The source of routing security problems lies in the way routing data are shared among ISPs. While most operators have an incentive to cooperate, existing data sharing and governance methods mean that there is a real problem with information validation.

We begin with some basic vocabulary. Routing announcements are statements broadcast by a network operator from its external gateway router to other operators’ routers using the BGP. Announcements contain the ASN, which uniquely identifies the network
making the announcement, and an IP address prefix associated with a node on the network. *Routing policies* are goals held by the router’s owner that control which routes are chosen and which routes are propagated to neighbours (Caesar and Rexford 2005, 5). ISP and other network operator-supplied inter-domain routing policies are stored in *routing registries*. Together, these registries comprise a shared, global view of routing policy information, which in aggregate is referred to as the *internet Routing Registry* (*IRR*) system. This information is ostensibly used by other operators to configure their network’s router filters, allowing them to validate some route announcements, and discard others that are invalid, by comparing them with routing policies (Butler et al. 2010).

The use, interaction, and governance of these data components (announcements, policies, and registries) are essential to ensuring accurate routing. In theory, routing registries should contain an accurate view of operators’ intended routing policies. In practice, however, network operators have different, and often conflicting incentives to supply or use data in the IRR system.

### 3. Existing forms of routing data governance

In this section, we will introduce two institutional forms that play a role in routing: IP address registries and IRRs. We will briefly refer to address registries, and then explore in some depth the incentive structures around IRRs, as well as exchanges of routing policy data among network operators.

#### 3.1. Authoritative institutions for globally unique identifiers (RIRs)

Between 1991 and 1997, Regional internet Registries (RIRs) were established, and in 2000 and 2005 two new ones were created.¹ RIRs are authoritative institutions for allocating and assigning the globally unique identifiers used in internet routing (IP address numbers and ASNs) (Mueller 2010). Network operators acquire exclusive use of specific IP address prefixes and autonomous system (AS) numbers from the RIRs, who maintain a registry that identifies specific numbers with specific organisations or users. A Whois service, which allows anyone to input an IP address or ASN and see the organisation to which it is registered, makes that information publicly accessible. Each RIR develops its own policies to govern the allocation, assignment, and use of IP and AS number resources. In short, RIRs solve the problem of ensuring the global uniqueness of IP address and ASN assignments by establishing centralised and authoritative hierarchies for their assignment. They also maintain directories that effectively link these authoritative resource allocations and assignments to specific entities. However, the number registries have no operational control over routing policies and practices. Ergo, RIRs are not the only potential source of routing security problems.

#### 3.2. IRRs and the sharing of routing policy information

Less well known than the RIRs, IRRs also came into existence during the formative period of internet governance in the early to mid-1990s. The IRRs can be described as a set of databases where network operators voluntarily share their routing policy information. This includes operator contact, route, ASN, resource-set, router, and other data objects,
in a semi-standardised format based on the Routing Policy Specification Language (RPSL). Policy information contained in IRRs can be used by operators to configure routers. In practice, an operator might automatically retrieve RPSL objects from the IRR system, convert that data into instructions that are understood by router software, and distribute those instructions to their routers. Policies may affect how routers filter (i.e. eliminate from consideration) imported routes, determine the most desirable route, or specify to which neighbouring ASs a route might be exported (Caesar and Rexford 2005, 7).

The routing registry model originated in the early 1990s, with operators’ routing policies first represented within the RIPE database in 1993. In 1994, in North America, the National Science Foundation awarded the Routing Arbiter Database (RADb) contract to Merit, Inc., a non-profit education and research networking association in Michigan, USA (Merit Network 1996). When the NSFNet was privatised and multiple ISPs started to exist, the single, centralised routing registry evolved into a diverse, open, networked data governance structure.

The supply of IRRs is decentralised and diverse. There is no inherent limit on the number of IRRs, and any entity can decide to provide one. None of them are authoritative or sanctioned by laws or regulations. Some IRRs are operated as specialised, stand-alone registries (RADb, ALTDB). Some are run by national or regional IP address registries. Some are run by internet service, hosting, or network security providers. The largest (in terms of data), oldest, and most oft-mirrored registry is the RADb maintained by Merit Inc., which inherited its prominent status from the NSF era. The number of operational registries fluctuates. Previous work looking at the evolution of the IRR system identified as many as 68 IRRs (Khan et al. 2010) operated by various organisations. Of these, we found 27 of the databases currently being updated. Table 1 shows the operational IRRs as of February 2016.

No one seems to make money on IRRs – at least, not compared to the way domain name registries charge profitable recurring fees for a unique name registration, or the way RIRs generate millions in annual revenue by charging membership dues and fees for leasing out unique number blocks to network operators. The stand-alone RADb, alone among IRRs, charges a $495 annual fee for commercial registrants, and a $395 annual fee for non-profit registrants. The data that users pay to enter into the RADb are not kept private, however; it can be copied (mirrored) by any other IRR or anyone else who wants to use it. In general, IRRs are not structured as a service paid for by users of the data, and thus they do not limit access to their data to paying customers. Once the data are entered, they are treated as a public good.

### Table 1. Internet routing registries.

<table>
<thead>
<tr>
<th>Organisation type (count)</th>
<th>Registry operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet service provider (13)</td>
<td>REACH, LEVEL3, GT, EPOCH, BELL, NTTCOM, AOLTW, BBOI, EASYNET, HOST, OPENFACE, PANIX, ROGERS</td>
</tr>
<tr>
<td>Hosting service provider (2)</td>
<td>SAVVIS, NESTEGG</td>
</tr>
<tr>
<td>Internet address registry (6)</td>
<td>AFRINIC, ARIN, RIPE, JPIRR, APNIC, TC</td>
</tr>
<tr>
<td>Stand-alone routing registry (2)</td>
<td>ALTDB, RADB</td>
</tr>
<tr>
<td>Research and education network (1)</td>
<td>CANARIE</td>
</tr>
<tr>
<td>Internet exchange point (2)</td>
<td>OTTIX, RISQ</td>
</tr>
<tr>
<td>Other (1)</td>
<td>RGNET</td>
</tr>
</tbody>
</table>
Many of the registry operators in the IRR system implement mirroring. For instance, Merit currently mirrors data from 28 other routing registries.\(^6\) This practice facilitates the discovery and availability of routing policies, as operators may use different registries. However, mirroring does not ensure consistency of route policies between the various databases.

### 3.3. IRRs as a broken data governance structure

The economic incentives underlying the input and usage of routing data into IRRs are unexplored in the literature. This section will examine the complex incentive structure among participants in IRRs, and show how these lead to many of the known inadequacies of IRRs as a tool for ensuring secure routing. In doing so, it will provide a rubric for evaluating other proposals.

In theory, IRRs become ‘better’ (more useful) by attracting more registrants and having the most accurate data about their routing practices. The key issue for routing security, therefore, is the completeness and accuracy of the data in an IRR, and the incentives for operators to utilise that data. Overall, we see IRRs as a flawed governance structure\(^7\) because they are characterised by: (1) misaligned incentives; (2) high transaction costs; and (3) unmanageable interdependencies.

#### 3.3.1. Misaligned incentives

Given current institutional structures, the incentives of the many actors involved in an IRR are not well aligned:

- Some operators claim reluctance to publish routing policies because it can reveal business relationships. For example, while an operator may be open to revealing it is a customer of a certain provider, providers are unlikely to reveal the customers for which they compete. It is important to note that routing policies do not necessarily reveal details of business relationships, and that AS path construction providing connectivity between operators can be distinct from business relationships. Nonetheless, some actors do not want to even reveal connectivity to another operator via publication of routing policies;
- Participation in an IRR could be seen as a classic collective action problem, leading to underproduction of a public good. The value of the IRR to filtering depends not only upon one’s own efforts, but also on the actions of dozens or even hundreds of others, which any individual user cannot predict or control;
- There are weak incentives to delete obsolete objects, as it involves work and no immediate benefit to the deleter;
- Failure to identify, update, or correct one’s own obsolete data affects others more than it affects the data source. It minimises an operator’s workload, for example, to publish all routing policies that they may use, even policies covering resources that are not currently announced. Nonetheless, the presence of data concerning unannounced resources can cause bloat and inconsistencies in IRR data.
3.3.2. High transaction costs
Even given a willingness to utilise the IRRs, doing so can involve high transaction costs:

- RPSL is notoriously difficult to use, and is not uniformly standardised;
- There is no systematic way to identify obsolete routing policies ex ante;
- It is difficult to verify the authenticity or accuracy of others’ routing policy data;
- Widespread mirroring across IRRs can be explained as an attempt to economise on transaction costs by simply copying entries generated by others, but does nothing to make the data consistent or more accurate;
- Routing anomalies are more likely to occur in larger ISPs with more interconnections (Kuerbis, Mueller, and Maulana 2015), but these larger ISPs are the least likely to be filtered systematically, because of the cost and effort required to configure filters for large ISPs, which have more numerous and frequently changing announcements.

3.3.3. Unmanageable interdependencies
Collective reliance on data that can be unilaterally altered creates unmanageable dependencies:

- Once IRR data have been used by a variety of uncoordinated actors to generate route filters, a unilateral change in the registry data by one party can have unexpected or undesired operational consequences.

   Based on semi-structured interviews with twenty network and IRR operators, conducted at regional network operator meetings, we elaborate on these problems below. Incentives to produce and use IRR data vary across multiple aspects, such as differences in operational needs, the routing problem being addressed, and registry limitations. The number of routing policy changes an operator makes can vary dramatically. A large ISP or internet Exchange Point with thousands of customers will make changes more frequently than a stub network, which may only change its routing policies once a decade. Many stub operators we interviewed had never dealt directly with the IRR system. On the other hand, several large operators require their customers to either use their own routing registry, or another registry which they mirror. To facilitate this, some operators communicate directly with customers and make changes to routing policies in the IRR for them (known as creating a ‘proxy registration’). Smaller ISPs may require their customers to enter data into the IRR. On the other hand, some operators’ customers may be willing to enter and maintain their own routing policy information, or even insist upon doing so.

   Incentives to use IRR data for filtering vary by operator type. According to one large US-based ISP, filtering of larger networks is very difficult and involves trade-offs. For example, to avoid the costs of constructing complex filters, some operators only filter announcements from smaller ASs, where route changes are less frequent. A large European ISP said that only a handful of large peering ISPs do ‘strict filtering’, that is, the filtering of every announcement. In their opinion, others do not do it for a variety of reasons, for example, too many changes from customers, or too much work. Small stub networks might not engage in filtering at all, relying instead on their upstream service provider to filter bad announcements.
Network operators and registry operators have few incentives to remove obsolete registry objects, and in some cases they have incentives not to. Some operators take a ‘set it and forget it’ approach to their routing activities, and unless there is an immediate impact on operations, they will take the same approach to routing policy data in the IRR. One Canadian operator considered cleaning up its registry objects, but was reluctant to delete objects because of potential unanticipated consequences. Furthermore, operators store ‘backup’ routing policies in the IRR that are not actually being announced. Likewise, non-ISP registry operators can be reluctant to remove objects (or cannot do so due to their terms of service) from the registry, for fear of possible impact on their customers’ operations. These potential operational and legal challenges highlight a simpler and more surprising problem: there appears to be no systematic way within the IRR system to identify routing policies that are obsolete or not currently being announced. Obsolete or incorrect data affect operator incentives to use the IRR.

3.3.4. IRR data accuracy and governance

A handful of studies have examined data accuracy in the IRRs. Early efforts attempted to determine the level of ‘data correctness’ in the IRR system by comparing IRR data to observed BGP announcement data. According to Siganos and Faloutsos (2004), RIPE operated ‘by far the most accurate registry’ but, overall, only ‘28% of the ASs have both a consistent policy and are consistent with BGP routing tables’. The accuracy of the RIPE data has been confirmed recently, with around 90% of the observable structure appearing in the registry (Gray and Mansoor 2015). Other efforts (Khan et al. 2010, 2013) categorised different types of objects observed in the registries, accounting for differences in operator types and their routing practices. Khan et al. (2013) developed data accuracy measurements for 14 registries, and noted that ‘the quality of the IRR data can vary significantly depending on the [routing registry], RIRs (to which ASs belong), and AS types’. For each registry, they identified the percentage of route objects that (1) directly matched BGP announcements (Direct-POM); (2) are considered ‘proxy registrations’, where a provider registers the route objects of their customers (Mntnr-POM); and (3) do not match BGP announcements, but can be explained by ‘legitimate’ inter-AS routing practices (AS link-POM), as shown in Table 2. Given the diversity of organisations operating routing registries, one should expect to see differing governance practices. Table 2 relates the data regarding IRR accuracy from Khan et al. (2013) to observed differences in the governance of the registries, which we collected through examining IRR documentation and interviews.

The data indicate that ISPs attempt to overcome the incentive problems and internalise collective action externalities by assuming responsibility for entering and updating their customers’ data. Five of the top six highest levels of proxy registrations (‘Mntnr-POM’ in Table 2) occur in registries operated by ISPs. Only one registry, operated by NTT, has both high levels of proxy registrations and a high level of direct matches between route objects and announcements. As one might expect, address registries, which are not involved in routing operations, maintain the lowest levels of proxy registrations. Our interviews with operators confirmed that service providers were often responsible for maintaining their customers’ routing object data. Presumably, operators (1) have the permission of their customers to enter objects (and associated resources) on their behalf and (2) are protected by their contract from creating objects for their customer with resources that are unauthorised.
Table 2. Data quality and governance of select IRRs.

<table>
<thead>
<tr>
<th>Routing registry</th>
<th>Khan et al. (2013)</th>
<th>Require customers to enter data</th>
<th>Restrict who can enter data</th>
<th>Authenticate data suppliers</th>
<th>Verify address and AS resource authorisation</th>
<th>Allow proxy registrations</th>
<th>Authenticate users of the data</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPIRR</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>BELL</td>
<td>0.92</td>
<td>0.02</td>
<td>0.01</td>
<td>0.95</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NTTCOM</td>
<td>0.6</td>
<td>0.2</td>
<td>0.07</td>
<td>0.87</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RIPE</td>
<td>0.78</td>
<td>0.04</td>
<td>0.04</td>
<td>0.86</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RADB</td>
<td>0.61</td>
<td>0.12</td>
<td>0.09</td>
<td>0.82</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>TC</td>
<td>0.81</td>
<td>0.0</td>
<td>0.01</td>
<td>0.82</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>APNIC</td>
<td>0.7</td>
<td>0.1</td>
<td>0.01</td>
<td>0.81</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ALTDB</td>
<td>0.52</td>
<td>0.18</td>
<td>0.11</td>
<td>0.81</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ARIN</td>
<td>0.52</td>
<td>0.04</td>
<td>0.21</td>
<td>0.77</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LEVEL3</td>
<td>0.43</td>
<td>0.12</td>
<td>0.22</td>
<td>0.77</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GT</td>
<td>0.34</td>
<td>0.23</td>
<td>0.16</td>
<td>0.73</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>REACH</td>
<td>0.11</td>
<td>0.14</td>
<td>0.46</td>
<td>0.71</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SAVVIS</td>
<td>0.39</td>
<td>0.13</td>
<td>0.17</td>
<td>0.69</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EPOCH</td>
<td>0.33</td>
<td>0.22</td>
<td>0.13</td>
<td>0.68</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: We have been unable to find data for empty cells. In some cases, however, it appears that registries with many empty cells are no longer operational or updated. For instance, while the RADb mirror indicates the BELL registry is updated, the actual data file indicates it was last updated in 2000. GT was acquired by Bell Networks in 2004, REACH is now a subsidiary of Telstra, and EPOCH was acquired by Megapath which operates its own registry.
While most IRRs allow proxy registrations, they differ in whether or not they verify who is authorised to use the resources identified in the route object. None of the registries with high levels of proxy registrations verify whether the entity entering the object is authorised to use the resource. Most of the address registries, with the exception of ARIN, verify that the entity entering an object is authorised to use the resources.

Objects referencing unauthorised resources are sometimes created. For instance, Clayton (2015) discovered objects in the RIPE routing registry which included references to unallocated address prefixes. According to him, the objects were created by spammers so that network operators would not filter their routes. Interestingly, RIPE does require authorisation from the resource holder before objects referring to those resources can be registered, but only for resources allocated by RIPE. According to one interviewee, inaccurate data in RIPE’s routing registry largely stems from fact that ASs which have IP address allocations from RIPE (and therefore authorisation to register route objects) may also register objects in the database for resources allocated from other RIRs. These are large, transnational operators that prefer to register objects in a single routing registry. No RIPE policy is currently in place to prevent these registrations and/or to validate resources allocated by other registries.

Arguably, any routing registry system serving network operators must allow for proxy registrations, but also provide authentication so entries are unforgeable and accountable. However, it does not necessarily need to provide resource authorisation, as that information can be validated using RIRs and other address registries, or is a condition of the contractual arrangements between service providers and customers.

4. Existing data governance alternatives for routing security

The internet’s ‘global routing table’ is essentially a decentralised, distributed ledger of route announcements (i.e. a statement of an AS number and IP address prefix where a resource can be reached), with each network operator maintaining its particular view of internet routing. Currently, an operator’s view of these announcements can be validated using data in the IRRs. As noted above, however, the IRR system suffers from individual incentive and collective action problems. Not all operators supply information to the IRRs, the accuracy of the information that routing registries maintain varies, and there are a variety of practices that govern registry data. As a result, not all operators use the information in the IRRs to configure their filtering, and those that do sometimes face problems such as stale data.

How can these problems be addressed? Some proposed solutions, such as RPKI and BGPSEC, would give operators the ability to authorise and validate resources used in route announcements by relying on more centralised and hierarchical data governance grounded in the RIRs. Other solutions suggest private ordering responses among operators and route-monitoring services.

4.1. RPKI, BGPSEC, and the IRRs

Siddiqui et al. (2015) provide a comprehensive review of RPKI and BGPSEC technologies and the routing security problems that they could solve, as well as challenges they face in adoption. It has been long known that operators face mixed incentives when it...
comes to the implementation of RPKI (Kuerbis and Mueller 2011). Computer scientists have detailed how ‘whacking’, or revoking a certificate in the RPKI could potentially disrupt an operator’s routing (Cooper et al. 2013). This problem can be caused by technological and operational mistakes, for instance improper configuration, or the expiration of a certificate. It could also be attributable to legal pressures an RIR might face.12 Wählisch et al. (2015, 6) ascertain that certain types of operators (e.g. content distribution networks) are inclined not to publish information in an RPKI because it reveals business relationships, or could hinder their use of denial of service attack mitigation services. Some operators we spoke with claimed their organisations are unable to sign terms of service agreements which indemnify RPKI operators (e.g. ARIN). Nonetheless, a limited number of operators are creating ROA data.13 One operator has gone so far as to automatically retrieve and validate ROAs from RPKI for prefixes of its customers and peers, and import that data in RPSL format to the IRR. In their opinion, this allows operators relying on their route policy information to have some level of assurance that route object data are correct. This would be consistent with Goldberg’s (2014) observation ‘that the combination of RPKI with prefix filtering could significantly improve routing security’. It is also consistent with Merit’s suggestions for integrating RPKI data with the IRR (Karir and Blunk 2011).

Although currently still being standardised, BGP Security (BGPSEC) allows operators to validate announcements along the AS path (i.e. not origin announcements as above). Likewise, it uses public key cryptography to add digital signatures to sequences of route announcements, which can be validated by operators. BGPSEC also faces many challenges. As Goldberg (2014) notes, it introduces additional complexity and costs by requiring real-time cryptographic validation by routers, and it also requires adoption by every AS on a given path before it is effective. Siddiqui et al. (2015) review the estimated hardware and software burdens on operators, including increased CPU load, memory requirements, and significant changes to how routers implement the BGP. Moreover, they note a study by Gill, Schapira, and Goldberg (2013) which surveyed ISPs, and found only 9% of those surveyed would prioritise security of AS paths over other operational considerations.

Operators we interviewed confirmed many of the challenges identified above concerning RPKI and BGPSEC. One large ISP said they would implement a hosted RPKI instead of using the RIR’s RPKI. They would also not implement BGPSEC completely on their routers (i.e. automatically discarding routes if they are not valid), but instead use signed route data to check against route announcements. Another operator of a financially successful global social networking platform stated that if their company could not justify the costs to upgrade its routers to support BGPSEC, then it was hard to imagine small ISPs or global transit providers operating on small margins being able to do so.

Crucially, the origin and path validation provided by RPKI and BGPSEC would not address certain routing security problems (Goldberg 2014; Huston 2015a). For instance, Huston (2015b) says that neither RPKI nor BGPSEC would have prevented a recent large route leak by an ISP:

The problem was that otherwise valid routing information was re-advertised to neighbours who did not expect to hear those routes. A customer of a network was re-advertising transit routes, and without some additional knowledge of routing policy concepts such as ‘transit’, ‘customer’ and ‘peer’, then the routing system cannot automatically [detect] such lapses in the integrity of implied routing policy.
Huston goes on to suggest that IRR use (and presumably filtering based on data in it) could have prevented the incident. Nevertheless, he also calls attention to the many problems plaguing the IRR system, including the technical inability of RPSL to describe per-session AS connections, routing registry data accuracy and related authentication and authorisation issues, number and coverage, and operator participation in registries.

In summary, RPKI and BGPSEC focus on authorisation of resource use and router announcements, introduce new costs and possible vulnerabilities, and do not resolve certain routing problems. Moreover, RPKI and BGPSEC are also reliant on a registry (or registries) of public key information to enable validation of resources and route announcements. This raises the question of whether or not they may also be susceptible to similar underlying misaligned incentives, transaction costs, and unmanageable interdependency problems associated with the IRR.

### 4.2. Private ordering responses to IRR failure

Network operators are utilising other services instead of the IRR. Several operators interviewed use commercial route-monitoring services to detect unauthorised use of their resources. What distinguishes these paid services from the IRR is that the operator provides its routing policy information directly to the service, in exchange for route monitoring. The operator’s routing policy information is compared with observed BGP announcements, and alerts are sent when anomalies occur. In other words, the route-monitoring service provider has faultless information about an operator’s routing policies. From an economic perspective, they turn the functionality of the public, shared good (IRR) into a private good sold to the network operator. The fact that the operator is paying for the service strengthens its incentive to provide accurate, complete, and up-to-date information about themselves to the service provider. Moreover, an operator’s routing policies remain confidential, rather than being published in open databases. Somewhat tellingly, Merit (operator of the RADb) recently began offering route asset monitoring to its customers. RIPE has also recently revamped its BGP monitoring system, and is considering offering the data to its members.

In another example of a private ordering alternative to the IRR system, one large US-based service provider ingress filters its downstream customers’ announcements, to ensure that they do not accept and propagate route leaks (where an AS path contains ASs of the provider’s peers). However, it does not rely on IRR data to configure those filters. Rather, it relies on direct communication with its customers, and a route announcement monitoring tool developed by another large operator that identifies route leaks among its peers. According to the ISP, it has effectively eliminated route leaks from its network.

### 5. Data governance alternatives for routing security

This section will evaluate two additional ideas to address the routing security problem. Firstly, we will examine the Mutually Agreed Norms on Routing Security (MANRS) initiative, an effort to influence operator behaviours with regard to routing security. Secondly, we will explore the idea of applying blockchain technology to the publication and distribution
of routing policies. We will then evaluate each solution in light of our previous economic analysis of the IRR system.

5.1. A normative approach to changing operator behaviour

The MANRS initiative\textsuperscript{16} was formally established by ISOC in 2013. Having evolved over several workshops and roundtables involving operators beginning in 2009, MANRS asks operators who sign up to the initiative to implement a set of practices to help improve routing security. These practices include preventing the propagation of incorrect routing information by setting, validating, and enforcing the routing policies of adjacent networks (via filtering), and validating operators’ authorisation to utilise address resources, among other activities.

Shared norms have long played an influential role in internet governance. Arguably, the success of these have been due, in part, to the relative homogeneity of the operator community involved. However, as diversity increases, it becomes increasingly difficult to arrive at norms to which all participants can subscribe, due to conflicting operational, legal, economic, and political interests or constraints. In such an environment, community enforcement of norms is challenged. ISPs’ ability to abide by shared norms may also be constrained by states, which are more likely to be unable to develop and conform to norms (Hurwitz 2014).

5.2. A blockchain for routing policy data?

As explained above, existing data governance alternatives for routing security have shortcomings. A way to more fully accommodate the distributed nature of routing policies while achieving agreement on their ‘ideal state’ is needed. Looking more generally at systems of trusted attestations, APNIC’s Chief Scientist Huston (2015b) has noted that blockchain technology, such as that used by the cryptocurrency Bitcoin, does provide an alternative to more hierarchically organised systems such as DNSSEC, RPKI, or BGPSEC:

To what extent the increased complexity of such blockchain models obfuscates inherent vulnerabilities of such an approach is of course open to further consideration and debate, but it does represent a secure system of trustable attestations that does not require the imposition of trusted points of authority to seed the entire system.

In light of this, one solution to achieving an accurate view of distributed IRR data might involve the application of blockchain technology. A blockchain is an append-only ledger to which blocks of transactions are securely recorded. The key aspects of a blockchain are its ‘distributed consensus, provable timeline, and unforgeability’ (Shamir, as cited in Anderson 2016). A distributed consensus protocol, run by the nodes in the blockchain, allows the blockchain to converge on a uniform view of transactions (Bonneau et al. 2015). A provable timeline and unforgeability are implemented using a combination of public key cryptography and a computationally intensive hash function that allows parties to validate the authenticity and sequence of transactions (Narayanan et al. 2016).

Blockchains can be operated in a variety of ways, and focus on different types of transactions. Access in order to submit, read, or modify transaction data can be public (i.e. ‘permissionless’), or can be private, and limited to a predetermined list of entities (i.e.
Moreover, blockchains with different characteristics can be combined to achieve particular benefits. For example, a private, permissioned ‘sidechain’ may be linked to an open, publicly verifiable blockchain (Back et al. 2014). While early implementations of blockchains focused strictly on cryptocurrency transactions (e.g. Bitcoin), more recent blockchains allow the implementation of generalisable ‘smart contracts’ or ‘user-defined programmes that specify rules governing transactions … that are enforced by a network of peers’ (Delmolino et al. 2015, 1). For example, the Ethereum blockchain offers programmes implementing fungible tokens, crowdsourcing platforms, and autonomous organisations, all with user-defined levels of centralisation. Operational design and programmatic decisions impact the auditability and points of control in a blockchain.

Significantly, at least two aspects of blockchain technology, namely unforgeability and a provable timeline, have been considered by routing registry operators. As early as 2004, Blunk suggested that updates or queries to the IRR could be digitally signed using PGP or X.509 to allow the validation of data objects and/or users. There is an ongoing effort to standardise the process of timestamping and digitally signing RPSL objects using RPKI-issued cryptographic keys, which would allow operators to validate and determine the relative age of objects using a resource in at least one routing registry (Kisteleki and Haberman 2016). Furthermore, a technology known as Blockstack serves as proof of concept in applying blockchain to facilitate internet-scale decentralised naming systems. According to its inventors, Blockstack separates control and data plane considerations, keeping only minimal metadata (namely data hashes and state transitions) in the blockchain (their system uses the largest public blockchain, i.e. Bitcoin, to record overall state) and using external datastores for actual bulk storage of name records (Ali et al. 2016, 182). In other words, operators maintain their resource records with no central authority having control over them. A distributed protocol is used to achieve consensus among operators on the system’s overall state. One could envision a similar system being applied to routing policies.

Less examined are the role of incentives and distributed consensus in blockchains, and their potential application to the IRR. ‘Clever incentive engineering’ plays an important role in achieving consensus on blocks of Bitcoin transactions, with special nodes in its network (i.e. ‘miners’) being financially rewarded to operate servers that run a distributed consensus protocol based on showing proof of work. According to Narayanan et al. (2016), Bitcoin’s blockchain achieves consensus in spite of dishonest actors, because the protocol probabilistically prevents dishonest transactions from being in the blockchain. Over time, the risk of a dishonest transaction being included in Bitcoin’s blockchain diminishes as it becomes prohibitively expensive. A similar, although likely non-remunerative incentive system could be envisioned, with the creation of blocks of routing policy ‘transactions’ in an IRR blockchain. The operation of routing registries by some large ISP operators already demonstrates they have an incentive to aggregate valid routing policy data, which can be used for filtering. However, it is an open-ended question whether a distributed consensus protocol could work to determine the accurate state of routing policy data across multiple blocks. In some respects, designing a distributed consensus protocol for routing policy would be much easier than one for a pseudonymous currency like Bitcoin. This is because there are far fewer known entities that have to achieve consensus.

Table 3 summarises the shortcomings of the IRR system identified previously in Section 3, and analyses whether and how MANRS or blockchain technology applied to the IRR
could provide a possible solution to those shortcomings. While MANRS does not address most problems associated with IRR data, it does confront two issues: by fostering bilateral exchanges of routing policy data between an AS and its customers, and adjacent networks (and encouraging filtering based on this) the approach makes that data private to those actors, and reduces the level of collective action required. MANRS suggests that maintaining publicly documented routing data (presumably in the IRR) is an ‘advanced action’ for ASs. However, nothing in the endeavour specifically addresses the transaction costs or unmanageable interdependencies associated with that activity.

Applying blockchain technology to routing policy data potentially tackles several issues. Given blockchain design flexibility, it could be possible to make some routing policy data (e.g. an AS-SET) private, but also include a representation of this policy in a public blockchain. This could allow other ASs to know when the private routing policy changed without divulging the actual policy. While a blockchain-based IRR would still continue to require policy data from numerous operators in order to be effective, other advantages of the system would lower the costs of participating. Firstly, object authenticity and integrity could be assured by leveraging RPKI key data, as proposed by Kisteleki and Haberman (2016), or similar public–private key data to create authenticable policy objects. One could envision a smart contract which would periodically call a resource authorisation system (e.g. RPKI) and initiate the creation of a new route object if necessary. Secondly, given the permanent blockchain record, objects entered into it would never need to (or be able to) be deleted. However, since blockchains have provable timelines, it would be possible to determine if an object utilising a particular resource has been made obsolete by a new object. In addition, a permanent ledger avoids situations where deleting an object

<table>
<thead>
<tr>
<th>Economic issue</th>
<th>Existing IRR system</th>
<th>MANRS</th>
<th>Blockchain IRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misaligned incentives</td>
<td>No privacy of routing policies</td>
<td>Makes routing policies private to ASes exchanging data</td>
<td>Can make routing policies private to participants under certain implementations</td>
</tr>
<tr>
<td></td>
<td>Requires collective action among all operators</td>
<td>Reduces collective action to any specific AS + number of interconnected ASes</td>
<td>Emphasises collective action of routing registry operators; requires standardisation of distributed consensus protocol</td>
</tr>
<tr>
<td></td>
<td>Weak incentives to delete or update objects</td>
<td></td>
<td>Objects never deleted from registry</td>
</tr>
<tr>
<td>High transaction costs</td>
<td>RPSL inadequate, difficult to use</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No systematic way to identify obsolete objects</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No systematic way to validate authenticity or accuracy of objects</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No data consistency across registries</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filtering not scalable for large ISPs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unilateral changes to route objects can have unanticipated consequences for other operators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmanageable interdependencies</td>
<td></td>
<td>Objects never deleted from registry, but can be identified by timestamp as obsolete</td>
<td></td>
</tr>
</tbody>
</table>
inadvertently impacts another operator(s). The chief advantage of the blockchain approach would be agreement on the global state of routing policies that are maintained by multiple operators, unlike today where data may be replicated, and possibly conflict across different registries. However, achieving this will require the development of a distributed consensus protocol.

6. Conclusion

Reconceptualising the routing security problem as a data governance problem caused by a combination of misaligned incentives, high transaction costs, an inability to manage organisational interdependencies, and collective action problems, provides a more realistic basis for evaluating alternative solutions and technical ways forward.

While in principle technical solutions such as RPKI and BGPSEC could solve some authentication and authorisation problems that lead to insecure routing, examined in a broader context they also create their own collective action problems and misdirected incentives – and they do not even fix some of the routing security problems. Integrating RPKI and IRR data potentially improves the quality of routing policy data, and route-monitoring services incentivise operators to provide accurate routing policy data privately, but neither address the data governance issues identified above fully. Normative efforts like MANRS encourage bilateral, private exchanges of routing policy data to encourage filtering, but face numerous challenges with regard to evolving operator practices, diversity, and community enforcement, and do nothing to improve the IRR as a non-rivalrous, non-excludable source of routing policy data.

While there remain many open-ended questions around blockchain, for instance its scalability (Croman et al. 2016), the application of blockchain technology to the IRR system with unforgeability, distributed consensus, and provable timeline characteristics shows some promise in addressing many of the previously identified data governance problems in routing security. A BIRR confronts operators’ misaligned incentives, allowing the private exchange of routing policy data where necessary, possibly reducing the collective action required to route registry operators, and reducing the amount of data maintenance required by operators. It also deals with some of the high transaction costs and unmanageable interdependencies associated with the current IRR system. Building on the existing RPKI (or other resource validation key stores) provides a systematic way to validate the authenticity and integrity of policy objects. Obsolete objects could be readily identified given a BIRR’s permanent, sequential record. Inconsistent objects in today’s independently operated registries could be eliminated, with a uniform view of routing policies achieved through distributed consensus.

Notes

2. See https://tools.ietf.org/html/rfc1786 and https://tools.ietf.org/html/rfc2622 for a full description of the object classes and how policies are specified. We characterise RPSL as ‘semi-standardised’ because it is an IETF Proposed Standard, yet has been extended by operators (notably Level 3) to meet their particular needs.

4. http://irr.net/docs/list.html lists most known registries including the URL of their data repositories. A historical mirror of the RADB (ftp://ftp.host.net/host/dbase), and a security researcher’s website (http://www.vulnerabilityassessment.co.uk/routereg.htm) provided additional data on registries.

5. None of the IRRs limit access to their data, and only one authenticates users. See Table 2.


7. Our analysis focuses on the governance flaws of the IRR system, not on specific technical shortcomings. Concerning the latter, some IRRs do not have secure connections, and the information delivered in response to a query cannot be verified as accurate or complete.

8. Interviews were conducted with individuals attending NANOG 64, 65 and RIPE 71, including network and registry operators.

9. The interviewee said, ‘if an AS-set object gets deleted it might invalidate a legitimate route to an AS’.

10. ‘When creating a route object you must authenticate against multiple maintainers to verify that you have control over the ASN and address space you are referring to.’ https://www.ripe.net/manage-ips-and-asns/db/support/managing-route-objects-in-the-irr

11. The problem is actually bit more nuanced, as there is a RIPE policy that requires operators to create local non-authoritative copies of objects that use resources allocated by other registries. However, it is not easy to discern the difference between imported objects with no means of direct authentication, and other objects that are directly authenticable. The main point is that it is difficult to authenticate objects in the RIPE routing registry that utilise resources allocated by another RIR.


13. See current levels of ROAs at National Institute of Standards and Technology’s RPKI deployment monitor, http://www-x.antd.nist.gov/rpki-monitor/


15. http://puck.nether.net/bgp/leakinfo.cgi


17. Bitcoin’s blockchain is the canonical example of the former, while an example of the latter includes Hawk, see https://eprint.iacr.org/2015/675.pdf

18. https://www.ethereum.org/

19. Bitcoin’s consensus protocol relies on miners being the first to complete a proof of work. The protocol rewards the first miner to find a solution to a computational problem, but blockchains can implement other types of consensus protocols.

Acknowledgements

The authors would like to thank the Réseaux IP Européens Network Coordination Centre (RIPE NCC) Academic Cooperation Initiative for selecting the work to be presented at RIPE72, held on 23–27 May 2016, in Copenhagen, Denmark.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the U.S. National Science Foundation under Award Number SES-1422629.
Notes on contributors

Brenden Kuerbis is a Postdoctoral Researcher at Georgia Institute of Technology’s School of Public Policy, a collaborator in the internet Governance Project, and a former Fellow in Internet Security Governance at the Citizen Lab, Munk School of Global Affairs, University of Toronto. His research focuses on the governance of internet identifiers and the intersection of nation-state cybersecurity concerns with forms of internet governance. Kuerbis’ research has been featured in Circle ID, Forbes, Washington internet Daily and academic publications including International Studies Review and Telecommunications Policy, and in the book, Opening Standards: The Global Politics of Interoperability, by MIT Press. He received his PhD from the Syracuse University iSchool.

Milton Mueller is a Professor at the Georgia Institute of Technology, School of Public Policy, and internationally prominent scholar specialising in the political economy of information and communication. The author of seven books and scores of journal articles, his work informs not only public policy but also science and technology studies, law, economics, communications, and international studies. His books Networks and States: The global politics of internet Governance (MIT Press, 2010) and Ruling the Root: internet Governance and the Taming of Cyberspace (MIT Press, 2002) are acclaimed scholarly accounts of the global governance regime emerging around the internet. Mueller serves on the Advisory Committee of the American Registry for internet Numbers (ARIN), and was appointed in 2014 to the IANA Stewardship Coordination Group. He received his PhD from the University of Pennsylvania.

References


