The RPKI and Route Origin Validation: Advances in Deployment and Measurement

PhD Qualifier Examination - Critical Review

John Kristoff
Computer Science
University of Illinois at Chicago
jkrist3@uic.edu

ABSTRACT

Routing leaks and hijacks have plagued the Internet ecosystem since the late 1990's. These events, often unintentional, are recurring reminders of the risk the Internet infrastructure is subject to. The Resource Public Key Infrastructure (RPKI) has arisen as an important and necessary component to facilitate secure Internet routing. Many network operators are now publishing digitally signed certificates of address prefixes and their associated route origins into the RPKI. A smaller, but burgeoning community of operators have begun deploying route origin validation capabilities to limit the propagation of invalid routing information in disagreement with the RPKI. Now researchers are building systems and techniques to evaluate how the RPKI is being populated and used, drawing comparisons to other Internet infrastructure security services such as the extensions to the domain name system. Private and localized validation policy decisions pose measurement challenges for would-be secure routing surveyors however. Operator polling, passive observation of route updates, controlled route announcement experiments, and data plane analysis are among the common techniques devised to estimate deployment today. When operators and route collection tools incorporate route validation state in data collection systems, researchers will be able to enhance their methods further still.

1 INTRODUCTION

The Internet is a network of networks. Each network that forms the larger whole is commonly represented and referred to as an autonomous system (AS). To form a loop-free connected graph, an AS typically uses the border gateway protocol (BGP), the Internet routing standard defined by the Internet Engineering Task Force (IETF) request for comments (RFC) 4271 to connect to one or more other autonomous systems.[20] AS-to-AS routers exchange and relay reachability information using BGP update messages, which include one or more address prefixes, an associated origin AS identifier, and other attributes as appropriate.

BGP is unique among most common Internet standard routing protocols due to the varied and widespread use of local policy configuration options available at each router node and within an AS. Each AS therefore may form different views of the larger Internet topology by accepting, rejecting, relaying, or altering routing information. That is, while a loop-free topology remains a critical feature of BGP, the shortest path to any destination may be a secondary goal depending on local administrator policy. For example, one network may choose to reject or withhold a route update containing a particular AS deemed untrustworthy. To illustrate another common scenario, an AS may devalue routing information in order to prefer one path over another. These types of local policy decisions affect local path computations, but can also impose policy onto neighboring networks and beyond, narrowing the path selection decisions further downstream.

In addition to the added complexity local policy configurations imply, the data conveyed in routing update messages between BGP speakers come with no express means of authenticity. Therefore by default, as long as the BGP message is well formed, a routing update with invalid path data may find its way into the path computation process, wreaking havoc and corrupting the computed topology of one or more autonomous systems. How does a BGP receiver evaluate routing information when an autonomous neighbor is untrustworthy either due to accident or malicious intent? Approaches to protection from invalid routing data have varied, haphazardly dealt with in each autonomous system as a local policy decision. Consequently, overall Internet routing infrastructure robustness against invalid routing data varies widely from AS to AS. While a variety of solutions have been deployed, the Internet has lacked a comprehensive, standard approach to authenticating routing data distributed through BGP. Unfortunately, the threats of invalid routing data are not hypothetical.

In 1997, a unique set of circumstances coalesced at just the right place and time to cause a major disruption in the Internet routing system.[3] A small Internet service provider (ISP) both disaggregated and regenerated a large number of Internet address prefixes back into the Internet, making it appear as if the address prefixes in these routing updates all originated from the small ISP. These numerous and erroneous updates cascaded to many other networks. To many Internet router configurations the updates were accepted and used to recompute paths. Instead of traffic following the best path during this event, many of intended destinations covered by these updates became unreachable as routers started forwarding traffic towards the wrong ISP.

Just over a decade later, another widely observed routing anomaly impacted the popular YouTube streaming video service.[6] Pakistan Telecom, intending to block access to YouTube from within its network accidentally leaked a specific address prefix covering a portion of YouTube's address space in a route update to an upstream provider. This in turn propagated as a preferred path to many other networks. The proliferation of this update sent many of the world's YouTube users towards Pakistan Telecom, which appeared in the routing system as the best path, but effectively led to an Internet version of a black hole.

The aforementioned network infrastructure mishaps, commonly referred to as a *hijack*, are among the most popular in the history of Internet routing. However, events such these, even when less well known, recur with surprising frequency. Often these events can be classified as accidents, but there is evidence many anomalies have been intentionally malicious.[16] Whether the events are benign or costly, inadvertent or deliberate, mechanisms to limit their occurrence have been an ongoing area of research, experimentation, and development.

This paper evaluates the deployment and measurement efforts of a new approach to hardening the Internet routing system against illegitimate routing updates. The rest of the paper is organized as follows: In §2 the history of secure routing is divided into two distinct eras. The first era summarizes popular techniques and tools network operators have traditionally deployed to limit the spread of invalid or unwanted routing information. The second era includes the recent design of the resource public key infrastructure (RPKI), route origin validation (ROV), and related standards efforts that form the basis for the bulk of this paper. In §3, approaches to measuring the deployment of the RPKI and ROV from three recent research papers that represent the state of the art are summarized. In §4, this paper offers fresh perspective and criticism of the prior research under evaluation. In §5, an argument is made to include and leverage the route validation state of ROV-enabled networks in route monitoring systems to encourage deployment and enhance measurement. The paper concludes in §6.

2 BACKGROUND

Secure routing conjures up images of different solutions for different challenges. One might dream of mechanisms to thwart byzantine failure or the use of encryption to protect the privacy of routing data in transit. It may may suggest a series of access control best practices or sane configuration defaults on hardware. For the purposes of this paper, and in terms of BGP, this paper is particularly concerned with authenticating the origin AS in the AS path attribute and the authorization granted the AS to originate an associated address prefix in the update message. Attention therefore converges on a subset of technologies that arose out of the Secure Inter-Domain Routing (SIDR) working group in the IETF.

While a complete tutorial and history of approaches to secure routing on the Internet is beyond the scope of this paper, a brief review of popular approaches and technologies relevant to understanding the RPKI, route origin authorizations (ROAs), and ROV is provided. The reader is encouraged to review the references provided for additional detail.

2.1 Route Filters and Prefix Limits

Two BGP capabilities frequently used to limit undesirable or unexpected routing updates are route filters and prefix limits. A route filter is a list of one or more rules that evaluates a received announcement in a route update and decides whether to accept, reject, or alter the announcement for local route computation. A prefix limit is a threshold, an expected upper limit of prefixes a BGP neighbor is expected to announce to the receiving router. A breach of a prefix limit may trigger an alert or shut down the BGP peering session.

Listing 1: Example Junos route filter

```
policy-options {
    prefix-list rfc1918 {
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
    }
    policy-statement sanitize-bgp {
        term rfc1918 {
            from {
                prefix-list-filter rfc1918 orlonger;
            }
            then reject;
        }
    }
}
```

Network providers commonly use route filters to reject route announcements they never expect to see. For instance, if AS *49152* deems reachability to the IPv4 address prefix `192.0.2.0/24` undesirable, a route filter could be applied to reject any announcement for `192.0.2.0/24` or smaller overlapping prefix from other networks. See Listing 1 for an example BGP policy implementing a route filter to reject route announcements for any address space covered by IETF RFC 1918 prefixes.[17]

Route filters can range from the relatively simple to thoroughly complex. Most router implementations provide an ability to peek into almost all parts of the routing announcement and pass judgment in myriad ways. A creative operator may be able to prevent many invalid routing updates using an elaborate set of route filters, but achieving complete protection from all possible invalid routes would be a Herculean, if not impossible task. Nevertheless, route filters along with prefix limits have been two of the most common and widely deployed capabilities to limit invalid route propagation on the Internet today.[8]

2.2 Internet Routing Registries

Since the early years of BGP deployment, the Internet community identified the need for tools and a set of best practices to support the sprawling routing infrastructure. One of the early developments to support these early challenges was the design and creation of Internet Routing Registries (IRRs).[4] The IRR system was an outgrowth of the desire to express an autonomous system's routing policy, primarily for troubleshooting and documentation purposes. Tools to help automate the validation of routing updates against IRR data soon appeared. In fact, when the *AS 7007 Incident*[1] occurred a number of operators suggested that the use of a routing registry could have prevented the problem.

IRRs and IRR tools have been adopted by a number of networks, but the data has been of varying completeness and quality.[14] Perhaps the IRR system was ahead of its time, or maybe it hasn't struck the right balance of cost, consistency, ease of use, and utility for it to have become universally deployed as a routing security mechanism. It would take a number of years and a few proposals before a system focused solely on routing security would take hold.

[1] This is the name given to the routing event in 1997 described in this paper above. 7007 refers to the autonomous system number assigned to the small ISP originating the invalid routes.

2.3 S-BGP and soBGP

At the turn of the 21st century two extensions to BGP, S-BGP and soBGP, proposed the incorporation of cryptographic authentication into the routing system.[13][25] Both approaches specified a public key infrastructure (PKI) and both modified BGP to incorporate authentication signaling into the routing protocol. Neither approach gained sufficient traction to become deployed systems however. Nonetheless, their use of a PKI foreshadowed a system to come that would capture the imagination of operators and soon demonstrate promising levels of real-world deployment.

2.4 The RPKI

At the center of modern secure routing technology today is the resource public key infrastructure (RPKI), a distributed, hierarchical repository containing cryptographically signed objects such as attestations of autonomous systems associated with Internet address prefixes.[15] The RPKI is formally structured with each regional Internet registry (RIR) anchoring the repository with the allocated address space they are responsible for. Address holders work with their respective RIR to populate the RPKI or to coordinate a delegation of partial repository data further.

The RPKI could be thought of as cross between the IRR system and a PKI-based system like those of attempted by S-BGP and soBGP. The RPKI, like the IRRs, but unlike S-BGP and soBGP, is maintained outside of the BGP protocol itself. The RPKI leverages the fundamental principles of an X.509-based PKI for routing data like those from S-BGP and soBGP, but unlike the IRR, decrees a unified, hierarchical structure, anchored and supported by all RIRs as an integrated service offering. The initial objects populating the RPKI provide the means by which to perform route validation, an overview of which is covered below.

2.5 ROAs

Route origin authorizations (ROAs) are individually signed objects associating allocated address prefixes with an AS authorized to originate routes for these prefixes in the BGP system. Neither BGP route updates nor RIR address allocation records alone make this relationship explicit. With the RPKI system and the ability to populate it with ROAs, the Internet routing system now has the two key building blocks on the way toward a secure routing infrastructure.

A ROA can have only one origin AS associated with one or more prefixes. Each prefix can specify a *maxLength* value for the prefix, indicating the most specific prefix length the origin AS is authorized to announce. Like X.509 certificates, other attributes such as a digital signature and expiration time are associated with each ROA. See Listing 2 for an example ROA as recently published in the American Registry for Internet Numbers (ARIN) RIR operational test and evaluation environment.

2.6 ROV

Colloquially known as route origin validation (ROV), BGP-speaking routers can use the RPKI and ROAs to influence routing policy decisions when BGP route updates are received.[7] If a route update is covered by a published, valid ROA, a ROV-enabled router compares the origin AS and prefix length in the update with corresponding data found in the ROA. What a router will do when a route update experiences a ROV failure is a local policy decision, but most operators either decrease the preference for the route or reject it outright.[2]

Listing 2: Example AS 20130 ROA

```
ROA Name: DEPAUL AS20130
Origin AS: 20130
Validity Period: 02-12-2019 to 02-12-2029
Resources:
    2604:95C0::/32
    2620:0:2250::/48
    75.102.192.0/18
    216.220.176.0/20

-----BEGIN SIGNATURE-----
CphdY76ofLDDsBzKseuivh9fp8j8f95xZSQrs75MF+GU0nP5OKKtn
J6UvFLZH6L8YEWcxiGGuwTzgK0Puea+slXnXU+UgalmitqJOHwXbo
bAm7DCWou2wT2fIWqZHTUpX99/jFlSn34ozp2NFWJCT8ba4WlNgnI
sevnaeoe2KzEUbaawYCOskLU9B7aAPFhBHbuGGhQYpx08n3zLYj1R
MIOyOyl8NuSi3cfI0KbRZjhtIF3Pe9LebuqrwiBhRaFxzvFLM4g6z
Dff62/7Hnmt6PFio0Rn1UWPq2plDymT5peluCdDiL3M/DsGrEgqRf
wQKql16HuRKaZVoHa0cNWPdw==
-----END SIGNATURE-----
```

To implement ROV, network operators are expected to deploy a set of RPKI caches, sometimes referred to as validators, on their local network. These validators periodically fetch repository data from the designated anchors in RPKI hierarchy. The validators are then used in tandem with ROV-enabled routers, whereby routers load validated ROA object detail, suitable for use as part of the BGP policy processing rules setup by the local network operator.

The RPKI, ROA management, and ROV deployment has stirred the interest of standards bodies, networks operators, and vendors in recent years. Consequently, measuring the deployment of the RPKI and ROV based on published ROAs has attracted an equal amount of attention from the Internet research community. The next section will critically analyze some of this most recent research activity.

3 METHODOLOGIES

The RPKI infrastructure along with associated ROV capable validators and routers are still relatively new technologies. The base specifications were published in 2012. Deployment began in earnest shortly thereafter and by 2013 public monitoring emerged to monitor deployment and collect statistics.[18] An early research paper focused on identifying how the newly deployed RPKI was being used, paying particular attention to the quality of ROAs network operators created for their prefixes.[11] This work was among the first to consider whether routing data would validate against published ROAs. The authors performed an *offline* passive analysis, comparing a snapshot of published ROAs with a snapshot of routing data from the Route Views project.[19] Ever since, research interest in the deployment of the RPKI and ROV has begun to take shape. More deployment strategies and measurement studies are now appearing as common themes in networking and security

[2] As of February 11, 2019, AT&T began "dropping all RPKI-invalid route announcements" from peers[5] This was considered a major milestone that could help encourage other providers yet to deploy RPKI-based technology.

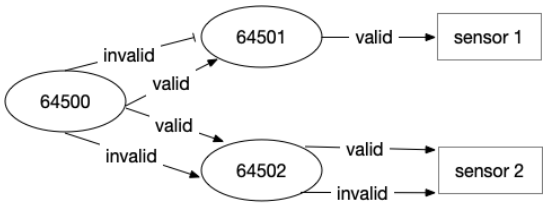

Figure 1: Passive ROV Detection

venues. This section explores some recent advances in deployment and measurement.

3.1 Uncontrolled Passive ROV Measurement

RPKI repository data, and specifically the ROAs, can be freely and easily retrieved. Normally the ROAs are ultimately fed to the routing system for ROV, but can be used to inform RPKI usage and measurement studies. Coupled with route collector systems such as those provided by the RouteViews project, researchers can study real-world data without having direct access to Internet routers. Inferences can be made from this passively collected data, but a hypothesis cannot be tested without a control variable present.

3.1.1 Method. Address allocations and ROAs are published in an open and transparent repository, a registry or RPKI respectively. ROV however is a local AS policy decision, unpublished in any central repository and generally unknowable to those unaffiliated with the local network administration. The authors in [9] propose a method to uncover ROV enforcement in the Internet by evaluating routes received at RouteViews sensors or vantage points. This study searches a sensor's collected data for an AS originating both valid and invalid prefixes when covering ROAs are published. The supposition is when both valid and invalid prefixes arrive at a sensor from a common origin AS, ROV is not enforced along the AS path.

Figure 1 demonstrates this inference approach. Two sensors see slightly different views of the topology. AS 64500 originates two prefixes, one valid, another invalid when evaluated with the RPKI. If AS 64501 is ROV-enforcing, only the valid route will be seen by sensor 1. Conversely, if AS 64502 is not ROV-enforcing, sensor 2 will see both valid and invalid prefixes.

3.1.2 Evaluation. In response to [9] another group of researchers found a number of limitations with this approach.[21] One set of problems stem from the nuances of local BGP policy decisions made by each autonomous system. For example, an AS that does not enforce ROV may receive and process competing invalid and valid routes, but may select the valid route as the best path for reasons unrelated to ROV. Only the best route will be propagated further, fooling an uncontrolled passive measurement approach. Another problem with this approach is that it requires the origination of an invalid route to detect whether or not an AS along the path is ROV-enforcing. An AS originating both valid and invalid prefixes may be a relatively rare event.

The authors in [9] claimed to have discovered nine of the top ISPs were enforcing ROV. However, [21] could not duplicate these results. The response paper attempted to recreate the measurement experiment and found the technique exhibited discrepancies dependent upon the RouteViews sensor data being evaluated. The original paper did not make their methods or specific data sources available so it was impossible to reconcile the differences seen between the two results.

Publishing ROAs, at least for address space that is not sub-allocated to downstream networks, is a relatively simple operation compared to ROV enforcement. It would stand to reason that an AS enforcing ROV is likely to also be publishing some ROAs, but the converse seems unlikely. Neither papers took into account whether any of the networks considered ROV-enforcing also had published ROAs. Only the[21] paper disclosed a list of autonomous systems they detected to be enforcing ROV. Historical ROAs are not readily available, but only two of the four networks identified as ROV-enforcing using a passive uncontrolled measurement approach have published ROAs as of this writing. With a controlled active measurement approach, detailed in the next section, the three networks identified as ROV-enforcing all currently publish ROAs.

3.2 Controlled Active ROV Measurement

Rather than rely on uncontrolled passive ROV measurement data derived from networks whose connectivity and BGP policy are largely hidden from view, a controlled experiment with active measurement could be undertaken. To measure ROV using this approach [21] proposes a series of experiments that start with a set of prefixes and ROAs under their supervision. Devising a series of experiments with these prefixes can produce direct observations that can in turn infer causation, leading to more reliable results.

3.2.1 Method. To observe ROV enforcement in the wild, researchers using this technique leveraged the PEERING testbed to originate two IPv4 /24 prefixes into the Internet BGP routing system.[23] Of the two prefixes announced, one is a control prefix whose announcement will always pass validation with a corresponding ROA. The other prefix oscillates between a valid and invalid state when its associated ROA changes during the experiment.

To minimize ambiguity about a network's ROV policy, only networks with vantage points (referred to as sensors by other researchers) and direct neighbors of the PEERING testbed are evaluated. Furthermore, each vantage point is verified at the start of the experiment to ensure it can see both prefixes with valid associated ROAs.

If a vantage point is unable to see the invalid experimental prefix or has a different route for the invalid prefix, the neighbor at this vantage is presumed ROV-enforcing.

3.2.2 Evaluation. This approach significantly improves the reliability of detecting ROV enforcement compared to the uncontrolled passive approach. However, this technique is limited in the number of networks it can evaluate since the PEERING testbed connects to a relatively small number of neighbors. The number of top ISPs connecting to the testbed is roughly 15% of the top 100. Nonetheless, the controlled active approach greatly improves the accuracy and robustness over an uncontrolled passive approach. The team from [21] identified three networks performing ROV using this method, all three confirmed this result when contacted. Conceivably this approach conducted on a larger scale, using larger well-connected

networks instead of just the testbed, could uncover a high number of ROV-enforcing networks.

This method might be susceptible to false positives if ROA propagation time, router recalculation behavior, or validator caching intervals are not considered. These researchers understood these potential problems and designed experiments to limit their effects by withdrawing a route before a ROA change and then subsequently issuing an announcement once the change was submitted. A potentially useful follow up study would seek to characterize ROA propagation behavior in the wild.

3.3 Data Plane Experiments

Thus far, approaches to ascertain ROV enforcement have centered on routing messages or routing table snapshots. These sources of insight derive from the network control plane. That is, this data collected says something about how the network is organized and the decisions individual routers purport to make, but taken in isolation does not say how data traffic actually traverses real world networks on an end-to-end basis. Furthermore, unless it were possible to compile a complete picture of the entire Internet routing system, there will likely be some disparity in the conclusions. Posed with these challenges, evaluation of ROV with the help of data traffic experiments, or the data plane, may enhance prior methods.

3.3.1 Method. The authors of [21] suggest in passing a way to extend the reach of their controlled active method when a vantage point is not available on a network peered with the testbed, but traceroute, reverse traceroute, or a RIPE Atlas probe is.[12][22] Data traffic would be sent from a candidate ROV network connected to the testbed network, towards a monitor on the origin AS. Observing the ingress peer interface for which trace traffic arrives, ROV enforcement could be observed.

In [10], the authors announce a pair of prefixes both originating from two distinct autonomous systems. A pair of ROAs for these prefixes are created. However, while each AS announces both prefixes, only one AS is valid for each prefix according to published ROAs at a time. Without ROV, it would appear as if the two prefixes are each multihomed to each AS or used in a common BGP anycast arrangement. For this experiment, traceroute probes towards the prefixes from RIPE Atlas probes are run. Each router hop from the traceroute output is translated to the associated AS originating a prefix for that router hop address. This in essence constructs a virtual data plane derived AS path. Inference for ROV enforcement is then made based on the networks seen or not seen in the traceroute data plane paths for a particular test prefix and destination AS.

The same authors devise a measurement approach where observation and control are available at only the origin AS end of the path. Here they evaluate SYN/ACK responses from TCP destination port 80 probes from test prefixes to Alexa top websites.[1] This method makes inferences about ROV enforcement when responses arrive at the invalid AS originating an associated prefix.

3.3.2 Evaluation. Using data plane inference to detect ROV is problematic. If the source and destination networks are peering neighbors, results can be reliable, but otherwise autonomous BGP policy decisions can mask a number of unforeseen reasons a router or network selects a best path. The authors of [10] acknowledge the uncertainty of their results and notably claim to prove only 0.1% of evaluated paths are ROV-enforcing. The authors did not disclose the networks detected as ROV-enforcing nor indicate whether administrators verified their findings. It is reasonable to retain some amount of skepticism without details of the findings, raw data, or manual verification.

The authors identify noise introduced with the traceroute data, such as packet loss. Other factors may influence the results, including inconsistent ROV enforcement within an AS, multihoming, traffic load balancing, and path asymmetry. Origin-only observation from SYN/ACK responses to probes is the least stable method. In this case, probes towards Alexa web sites may not all arrive at the same destination instance. Web sites may be distributed with a content distribution network, resulting in additional unfiltered noise. If different probes or responses traverse entirely different paths, filtering the results will be required, but difficult. The only observation is in the reply that returns to the source, which contains almost no path information other than the TTL (hop limit in IPv6) presuming the already unreliable record route option is not used.

Any claim of proof seems suspect unless the authors verified their findings with network administrators. They reason that an AS that only sees valid announcements and never invalid paths must be ROV-enforcing. They do not make available the code or data to recreate this experiment, so that this claim can be verified. The results from these data plane experiments verify even fewer ROV-enforcing networks than reported in [21]. False negatives with the data plane methods outlined here are likely higher. While the experiments are active and partially controlled, ambiguity is introduced when trying to evaluate ROV enforcement when there are multiple intervening AS hops in a path. It is difficult if not impossible to deduce with certainty routing policy that may exist between the different pairs of AS neighbors when measuring from afar.

3.4 Deployment Challenges

As of this writing, depending on how one counts, deployed ROAs cover approximately 10% to 15% of the IPv4 Internet. While a direct comparison cannot be made, signed DNSSEC zones see high levels of participation at or near the top of the name space, but is much more sparse below. Nonetheless, many zones have been signed, but compared to all possible zones, the coverage rate is about an order of magnitude smaller than ROAs. This may say more about the RPKI than DNSSEC. DNSSEC is a much older technology, but there is also much more individual DNS data to sign than routing data. ROV adoption on the other hand appears to still be in its infancy, but appears poised to see steady growth and increased coverage of the IP address space. While deployment of the RPKI, ROAs, and ROV enforcement is encouraging, barriers and difficulties remain.

3.4.1 Political, Economic, and Social Limitations. As reported in [26], not all deployment challenges are technical in nature. For instance, ARIN, the North American RIR, requires users of their portion of the RPKI to overcome strict legal obstacles spelled out in their terms and conditions agreements. Adoption in the ARIN region is believed to be artificially limited due to these legal concerns. Each RIR operates differently and these differences are sometimes

used to explain why ROA publication rates vary dramatically from one RIR to another. In fostering deployment of securing routing, RIPE is statistically ahead by a significant amount. In [2], it was demonstrated that a series of focused interface improvements and ongoing constituent engagement helped foster deployment of the RPKI in the RIPE community.

Perhaps the most cited deployment challenge with any new technology is achieving critical mass when participation is its own reward, but where there is little incentive for early adopters. Publishing ROAs is relatively easy, but there is little advantage in doing so if networks are not performing ROV. One suggestion by [9] is to encourage ROV deployment in the core of the Internet, by the largest ISPs. Their evaluation argues that with just a modest amount of ROV deployment in the core the value of ROAs increases are non-linear.

3.4.2 Technical Hurdles. New systems may experience failures or begin with low quality data as users and input are introduced. Invalid ROAs pose a particular problem as networks recoil from a technology if it is deemed not ready for production use. If an AS incorrectly populates the RPKI with an incorrect ROA and other networks are ROV-enforcing, the origin AS may suddenly find themselves disconnected from the Internet. This potential problem has convinced some networks to only depreference invalid routes rather than reject them outright.

Recent research has produced a number of monitoring systems to help detect and foster deployment. The Rov Deployment Monitoring (RDM) system from the [21] team publishes a regular report on ROV deployment as detected by their measurement methods. The RDM provides a searchable interface to explore the ROV status of observed networks. The [9] team has created the complimentary monitor known as ROAlert, which is concerned with the signed data, or ROAs. ROAlert highlights potential ROA usage deployment problems such as address sub-allocation dependencies.

A particular problem for large ISPs has been twofold. In publishing ROAs, they must take care to avoid invalidating more specific routes originating from customers. For instance, if AS 49152 is allocated 192.0.2.0/24 and publishes a ROA for that specific prefix, but then sub-allocates 192.0.2.128/25 to a customer 49153, the customer's announcement will appear invalid until a customer-specific ROA is published. Another problem is when an ISP enforces ROV and ends up rejecting routes that are invalid, but unintentionally so. While this may seem like a necessary trade-off, network users may often prefer connectivity over "doing the right thing". If a downstream network becomes unreachable or a downstream network is unable to reach something they care about due to ROV enforcement upstream, the downstream network may decide to connect to another upstream network that doesn't burden them with ROV enforcement.

One proposal to limiting the downward dependency conflicts is with the introduction a new wildcard ROA.[9] A wildcard ROA would allow an AS to create another lower priority ROA for an aggregate prefix without specifying a specific origin AS. The wild card would permit any other AS to announce smaller prefix from this aggregate, without first having to create a specific ROA of their own. This syntactical problem with this solution is that the asID field in a ROA is specified as an integer. What value would represent a wildcard? A special value representing the wildcard function would need to be assigned and then router implementations would need to know to recognize this value. The practical problem with this approach is that a wildcard may now permit any origin AS to bypass ROV enforcement for the associated prefix, including random malicious networks, posing a potential hijack risk. Notably, this solution seems to contradict the concerns raised by the proposers for so-called *loose* ROAs this paper discusses below.

3.4.3 Security Concerns. At present, secure routing technology using the RPKI, ROAs, and ROV is most helpful in mitigating accidents and mistakes, but is unable to thwart many intentionally malicious attacks. An evil AS could modify the AS path of a ROA-covered prefix to include a valid origin AS, but list itself as a network on the path. As long as the prefix announcement validates according to a ROA, ROV will not detect this malicious route announcement. All else being equal, this increased path length may limit its propagation, but it may be sufficient to hijack some traffic. Alternatively, the malicious originator could announce a more specific prefix if allowed by a ROA *maxLength* value.

One of the few specified fields in a ROA, *maxLength*, declares the smallest prefix length that may be announced for the associated address block. For instance, imagine a ROA prefix is 192.0.2.0/24 but allows a more specific announcement up to a /32, the prefix would be listed as 192.0.2.0/24 but the maxLength value would be 32. The intent of the maxLength attribute is to allow an origin AS some nimbleness to disaggregate prefixes without having to create and distribute additional ROAs. However, [9] warns of a potential problem if the steady state origin announcement uses the least specific original prefix length. A malicious origin could come along and inject a more specific prefix with the spoofed AS and pass ROV. This technically does not increase the risk of hijacking without ROV, but if the maxLength were not used, it would invalidate more specific prefix hijacking attacks. The routing community appears to be gravitating toward a stance of not using the maxLength field unless absolutely necessary.

In some scenarios, the deployment of ROV may lead to unexpected network partitions or paths. In partial ROV deployment scenarios, an ROV-enforcing network may or may not receive the protection it might expect.

Figure 2 recreates three possible scenarios described in [9]. *(a)* depicts the ideal scenario in partial ROV deployment. Here AS 64510 performs ROV and protects 64511 from the invalid route originated by AS 64496. In *(b)*, AS 64510 does not perform ROV, but the downstream AS 64511 does. AS 64510 receives seemingly equal path options for the same prefix, but happens to select and relay the invalid route to AS 64511. Unless AS 64511 has a default route through AS 64510 or another unseen path, it will be disconnected from the valid origin AS 64495 entirely. Disconnection may be preferable to forwarding traffic toward the wrong network however. Lastly, in *(c)* a hijack occurs when AS 64510 fails to perform ROV and relays a covering valid /24 prefix and a covering invalid, but also a more specific /25 prefix. AS 64511 rejects the invalid more specific, but it doesn't matter, because it sends traffic to AS 64510 matching the valid, but less specific prefix. AS 64510 will then forward traffic towards the more specific invalid path anyway.

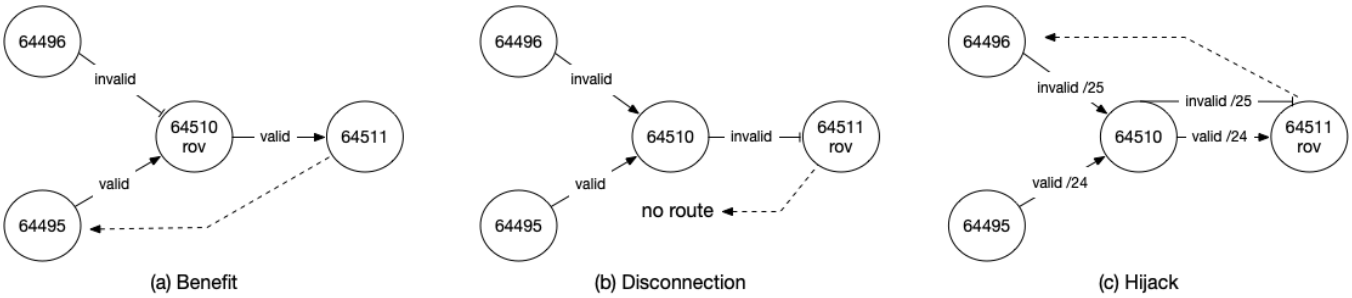

Figure 2: Partial ROV adoption scenarios

4 DISCUSSION

An Internet RPKI infrastructure to support secure routing is available and actively being deployed. Approximately 10% of active AS networks on the Internet have published ROAs in the RPKI. Research measurement studies attempting to uncover ROV enforcement deployment have uncovered very little use of ROAs to secure routing thus far. Nonetheless, interest in ROV deployment appears to be on the verge of growth given the recent rise in activity by operators and researchers. Meanwhile deployment challenges remain, stemming from hesitation by operators over technical and organizational policy concerns, ending with technical challenges involved in the roll out of most any new technology. Researchers have produced a handful of alerting and monitoring tools to help ease the transition to ROV and help validate proper ROA creation.

The earliest ROV measurement experiments utilized passive, uncontrolled routing data from route collectors such as RouteViews. While this source of data can provide insights, passive, uncontrolled inferences are prone to false positives and false negatives as a result of ambiguities in local AS routing policy along the route path. A controlled, active measurement technique decidedly improves the robustness of ROV measurement research. Observing controlled route announcements at nearby vantage points can produce reliable discovery of ROV enforcement on neighboring networks.

The research community has most recently proposed data plane techniques to detect ROV adoption on network paths. This effort can prove fruitful with limited short AS paths, but ambiguity increases quickly after the first AS hop. Data plane methods currently provide limited utility compared to the their control plane counterparts, suggesting more novel enhancements to this approach are needed to prove useful.

5 FUTURE WORK

Achieving insight from running networks at a distance is sufficiently difficult with existing measurement methods. Operators may be reluctant or unable to help provide direct access to their infrastructure for research experiments so researchers must devise innovate ways to uncover RPKI usage and ROV enforcement. Achieving additional visibility of ROV enforcement from deployed routers is currently only available by local administrators or through inference methods described above. While some inference methods such as controlled active measurement produce reliable results, they offer only a very partial view of the entire Internet secure routing posture. To better understand ROV enforcement as deployed in the Internet, route collection systems should explicitly mark routes with the local validity state.

Most modern routers maintain ROA validity state, but it remains hidden within each router. There are only three states, valid, invalid, or unknown. One approach would be to create a new, optional BGP, path attribute that could carry the validity state with an update. This might also be useful by downstream networks who would prefer to rely on the ROV mechanisms of their upstream provider, but it would be particularly useful for route collection systems such as RouteViews, significantly enhancing measurement studies. It is no small feat to alter the BGP specification however. To evaluate this approach a unique community tag could be used for this purpose initially.

The BGP Monitoring Protocol (BMP) is a new capability of many routers.[24] BMP exports routing table and peer status to a BMP collector. BMP in essence provides a remote, passive view of BGP state to a collector. BMP was designed to supplant and improve upon more rudimentary route collection systems that are often just *screen scraping* the output of commands that display routing information on a router. BMP is ideally suited to augment routing data collection with route validity state. It would seem practically feasible to extend BMP to include validity state in an extension or in a protocol update.

6 CONCLUSION

This paper considered a primary set of related papers on the deployment of secure routing using the RPKI and with a particular focus on ROV measurement methodologies on the Internet. A background of routing technologies and features that have traditionally been used to secure routing was covered in order to level set a discussion involving the modern RPKI-based environment. The design of the RPKI, ROAs, and ROV appear to have been influenced by lessons from previous technologies or secure routing proposals as deployment appears on a steady upward trajectory. Measuring just how deeply and widely ROV enforcement is occurring however is a challenge due to the inaccessible local policy decisions at each AS from would-be outside researchers. Nonetheless a handful of techniques have been devised to infer ROV deployment and enforcement activity with varying levels of reliability and reach. Controlled active measurement techniques are especially promising. To increase the breadth of ROV enforcement detection however, new techniques or sources of route validity will be required.

ACKNOWLEDGMENTS

John is grateful for the networking position he holds at DePaul University, which facilitates the ability to conduct meaningful experiments such as those in ARIN's operational test and evaluation environment (OTE) used to better understand the technology presented in this paper. John is also indebted to Patrick W. Gilmore, who generously made his time available to answer questions about the 1997 *AS 7007 Incident*.

REFERENCES

[1] 2018. Alexa. (2018). https://www.alexa.com
[2] Alex Band. 2015. RIPE Lessons from RPKI adoption. (Feb. 2015). https://www.nanog.org/meetings/abstract?id=2500
[3] Randy Barret and Steven Vonder. 1997. Routing snafu snips Net service. *Inter@ctive Week* 4, 13 (April 1997).
[4] Tony Bates, Elise Gerich, Laurent Joncheray, Jean-Michel Jouanigot, Daniel Karrenberg, Marten Terpstra, and Jessica Yu. 1995. *Representation of IP Routing Policies in a Routing Registry (ripe-81++).* Number 1786 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC1786 Published: RFC 1786.
[5] Jay Borkenhagen. 2019. AT&T/as7018 now drops invalid prefixes from peers. (Feb. 2019). https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html
[6] Martin Brown. 2008. Pakistan hijacks YouTube. (Feb. 2008). https://web.archive.org/web/20080228113848/http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml
[7] Randy Bush. 2014. *Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI).* Number 7115 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC7115 Published: RFC 7115.
[8] Jerome Durand, Ivan Pepelnjak, and Gert Doering. 2015. *BGP Operations and Security.* Number 7454 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC7454 Published: RFC 7454.
[9] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Shulman. 2017. Are We There Yet? On RPKI's Deployment and Security.. In *NDSS*.
[10] T. Hlavacek, A. Herzberg, H. Shulman, and M. Waidner. 2018. Practical Experience: Methodologies for Measuring Route Origin Validation. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 634–641. DOI: http://dx.doi.org/10.1109/DSN.2018.00070
[11] Daniele Iamartino, Cristel Pelsser, and Randy Bush. 2015. Measuring BGP Route Origin Registration and Validation. In *International Conference on Passive and Active Network Measurement*. Springer, 28–40.
[12] Ethan Katz-Bassett, Harsha V. Madhyastha, Vijay Kumar Adhikari, Colin Scott, Justine Sherry, Peter Van Wesep, Thomas E. Anderson, and Arvind Krishnamurthy. 2010. Reverse traceroute.. In *NSDI*, Vol. 10. 219–234.
[13] Stephen Kent, Charles Lynn, and Karen Seo. 2000. Secure border gateway protocol (S-BGP). *IEEE Journal on Selected areas in Communications* 18, 4 (2000), 582–592.
[14] Akmal Khan, Hyun-chul Kim, Taekyoung Kwon, and Yanghee Choi. 2013. A Comparative Study on IP Prefixes and Their Origin Ases in BGP and the IRR. *SIGCOMM Comput. Commun. Rev.* 43, 3 (July 2013), 16–24. DOI: http://dx.doi.org/10.1145/2500098.2500101
[15] Matt Lepinski and Stephen Kent. 2012. *An Infrastructure to Support Secure Internet Routing.* Number 6480 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC6480 Published: RFC 6480.
[16] Doug Madory. 2018. BGP Hijack of Amazon DNS to Steal Crypto Currency. (April 2018). https://internetintel.oracle.com/blog-single.html?id=BGP+Hijack+of+Amazon+DNS+to+Steal+Crypto+Currency
[17] Robert Moskowitz, Daniel Karrenberg, Yakov Rekhter, Eliot Lear, and Geert Jan de Groot. 1996. *Address Allocation for Private Internets.* Number 1918 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC1918 Published: RFC 1918.
[18] NIST. 2019. RPKI Deployment Monitor. (2019). https://rpki-monitor.antd.nist.gov/
[19] University of Oregon. 2019. Routeviews. (Feb. 2019). http://www.routeviews.org/routeviews/
[20] Yakov Rekhter, Susan Hares, and Tony Li. 2006. *A Border Gateway Protocol 4 (BGP-4).* Number 4271 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC4271 Published: RFC 4271.
[21] Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C. Schmidt, and Matthias Whlisch. 2018. Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering. *ACM SIGCOMM Computer Communication Review* 48, 1 (April 2018), 19–27. DOI: http://dx.doi.org/10.1145/3211852.3211856
[22] RIPE NCC Staff. 2015. RIPE atlas: A Global Internet Measurement Network. *Internet Protocol Journal* 18, 3 (Sept. 2015).
[23] Brandon Schlinker, Kyriakos Zarifis, Italo Cunha, Nick Feamster, and Ethan Katz-Bassett. 2014. Peering: An AS for Us. In *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*. ACM, 18.
[24] John Scudder, Rex Fernando, and Stephen Stuart. 2016. *BGP Monitoring Protocol (BMP).* Number 7854 in Request for Comments. RFC Editor. DOI: http://dx.doi.org/10.17487/RFC7854 Published: RFC 7854.
[25] Russ White. 2003. Securing BGP: soBGP. *Internet Protocol Journal* 6, 3 (Sept. 2003), 15–22.
[26] Christopher S. Yoo and David A. Wishnick. 2018. Lowering Legal Barriers to RPKI Adoption. *U of Penn Law School, Public Law Research Paper* 19-02 (2018).