Taking the Low Road: How RPKI Invalids Propagate

Ben Du
UC San Diego
bendu@ucsd.edu

Cecilia Testart
Georgia Tech
ctestart@gatech.edu

Romain Fontugne
IIJ Research Lab
romain@iij.ad.jp

Alex C. Snoeren
UC San Diego
snoeren@cs.ucsd.edu

kc claffy
UC San Diego
kc@caida.org

CCS CONCEPTS

• **Networks** → **Network security**; **Network measurement**.

KEYWORDS

BGP, RPKI, Route Origin Validation, Routing Security.

ACM Reference Format:
Ben Du, Cecilia Testart, Romain Fontugne, Alex C. Snoeren, and kc claffy. 2023. Taking the Low Road: How RPKI Invalids Propagate. In *ACM SIGCOMM 2023 Conference (ACM SIGCOMM '23), September 10, 2023, New York, NY, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3603269.3610843

1 INTRODUCTION

The Border Gateway Protocol (BGP) includes no mechanism to verify the correctness of routing information exchanged between networks. To defend against unauthorized use of address space, the IETF developed the Resource Public Key Infrastructure (RPKI), a cryptographically attested database system that facilitates validation of BGP messages. Networks can use RPKI to check whether the Autonomous System (AS) at the origin of the AS path in a BGP announcement is authorized to originate the IP prefixes being announced.

To be effective, RPKI requires two steps: (1) networks register their routing information in the RPKI; and (2) networks perform route origin validation (ROV) on received BGP messages (i.e. filter routes based on information in the RPKI). But operational and legal constraints have prevented full deployment. Only a subset of networks have registered in the RPKI [1, 2]; even fewer networks have deployed ROV [3, 5, 8]. Also, some networks, especially large transit providers, only partially deploy ROV due to complex business relationships.

We explore a lightweight technique to identify ASes that propagate RPKI invalid prefixes, *i.e.,* do not perform ROV. If the ASes responsible for propagating the most invalid prefixes were to deploy ROV, it could dramatically increase the security of the routing ecosystem. Thus, stakeholders can focus on promoting ROV deployment in those ASes. Our technique can help optimize future ROV deployment, *e.g.,* to estimate which ASes would provide the greatest marginal increase in protection.

2 BACKGROUND AND RELATED WORK

We classify BGP announcements based on their RPKI status. *Not found*: the announced prefix is not covered in RPKI. *Invalid ASN*: the origin AS of the BGP prefix conflicts with the AS of the matching prefix in RPKI. *Invalid prefix length*: the announced prefix is too specific compared to its matching RPKI prefix. *Valid*: the BGP prefix and origin AS matches RPKI. ROV-deploying networks drop *Invalid ASN* and *Invalid prefix length* BGP announcements.

In 2023, researchers estimated ROV deployment by sending traffic from multiple probes to two controlled prefixes (one *valid* and one *invalid ASN*) and found that 48% of probes reached the *invalid ASN* prefix [7]. They also identified the top 3 ASes that carried traffic toward the *invalid ASN prefix*. Our methodology differs in that we use only control-plane data (BGP routes) and provide a more generalized view of the propagation of RPKI-invalid prefixes.

ACM SIGCOMM '23, September 10, 2023, New York, NY, USA

ACM ISBN 979-8-4007-0236-5/23/09.
https://doi.org/10.1145/3603269.3610843

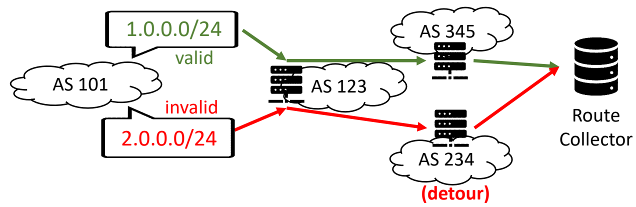

Figure 1: The RPKI-invalid prefix detours around AS345, propagating through AS234. AS345 performs ROV but AS234 does not.

3 DATASET AND METHODOLOGY

We use a one-week (1 July 2023 – 7 July 2023) snapshot of the Internet Health Report [6] that contains BGP prefixes, origin ASes, RPKI status, transit ASes, and AS hegemony scores. To compare differential treatment of valid and invalid prefix announcements, we consider only origin ASes that originate *both* RPKI-valid and RPKI-invalid ASes. For these ASes, we first quantify how many ASes propagate each type (RPKI-valid vs. RPKI-invalid).

How RPKI-invalids detour around primary transit ASes. By focusing on ASes that originate both valid and invalid prefixes, we can examine how invalid announcements propagate. In particular, invalid announcements may take a *detour* around the origin AS' primary transit providers because they filter invalids. We study this behavior by examining ASes that appear on the AS path of RPKI-invalid announcements but *not* RPKI-valid announcements. (Other ASes were preferred for RPKI-valid announcements.) Figure 1 shows an example where AS101 originates one RPKI-valid prefix and one RPKI-invalid prefix. Upstream AS345 deploys ROV and propagates only the RPKI-valid announcement. Consequentially, the RPKI-invalid announcement propagates differently and takes a detour to AS234 to reach the route collector.

Analysis of ASes that propagate announcements of all RPKI statuses. For transit ASes that propagate both RPKI-valid and invalid announcements, we use the IHR AS hegemony scores to analyze their relative prevalence in the corresponding AS-paths

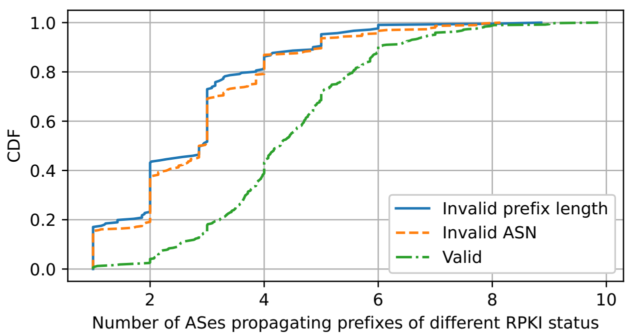

Figure 2: RPKI-valid announcements have more diverse transit ASes compared to RPKI-invalid ones.

of those announcements. The AS hegemony score is a metric that shows the likelihood of an AS to provide transit for prefixes [4]. For each transit AS, we calculate the aggregated hegemony score for all RPKI-valid announcements it propagates. We repeat the calculation for all RPKI-invalid announcements. Intuitively, a transit AS should be more prevalent in the path of RPKI-valid announcements, and thus have a higher aggregated hegemony score than that of the invalid announcements.

4 RESULTS AND DISCUSSION

RPKI status of observed announcements. In our one-week IHR snapshot of global routing tables, the median announcements for each RPKI status were as follows: 1,434 RPKI *invalid ASN*, 2,061 *invalid prefix length*, and 425,665 *valid*, and 525,080 *Not Found*. For our subsequent analysis, we focused on the 490 ASes that originated both RPKI-valid and RPKI-invalid announcements consistently for 7 days (63,184 *valid*, 773 *invalid ASN*, and 1,779 *invalid prefix length*). Of the 2,552 consistent invalid announcements, 1,929 (76%) were /24s and the 7 largest prefixes were /18s.

RPKI-valid announcements propagate farther across the Internet. For each AS, we calculated the average number of transit ASes of all announcements of each RPKI status. We found that RPKI-valid announcements had more transit ASes than RPKI-invalid announcements (Figure 2). This shows that enough ASes have now deployed ROV to cause a topological difference between the propagation of RPKI-valid and invalid announcements, a measure of the effectiveness of RPKI.

115 ASes appeared as backup transit for invalid announcements that primary transit ASes dropped.

We consider a transit AS *detour* if it propagated only RPKI-invalid announcements for at least one origin AS. Of 457 unique ASes that propagated RPKI-invalid announcements, 115 were such detour ASes. We found that 86 (75%) out of 115 detour ASes propagated only invalid announcements for only one origin AS. Only 4 detour ASes propagated invalid announcements for at least 10 origin ASes.

Table 1 shows the top 10 detour ASes that propagated RPKI-invalid announcements (*invalid ASN* or *invalid prefix length*) from the most origin ASes. We further studied the geographical distribution of the origin ASes that used those ASes for detour transit. We found that AS6762, a large transit provider, provided transit for invalid announcements from all 5 Regional Internet Registry

Transit ASN	Company	# AS	# Invalid Pfx
AS 6762	Telecom Italia	275	1,716
AS 6461	Zayo	62	217
AS 7473	Singapore Telecom	37	154
AS 6453	TATA America	22	77
AS 5511	Orange S.A.	9	112
AS 1273	Vodafone	9	34
AS 701	Verizon	8	64
AS 15412	Flag Telecom	8	38
AS 3320	Deutsche Telekom	5	16
AS 9304	HGC Global	6	10

Table 1: Top 10 detour transit ASes. Columns 3 and 4 show the numbers of origin ASes and invalid prefixes for which the detour AS provided transit.

(RIR) regions (RIPE, ARIN, APNIC, AFRINIC, and LACNIC). Similarly, large transit provider AS6461 propagated invalid announcements from four regions (all but RIPE) and Singapore-headquartered AS7473 from only the APNIC region. While large transit providers have complex routing and business ecosystems that may prevent full ROV deployment, this analysis provides a starting point for promoting expanded ROV deployment.

AS hegemony as a metric to guide deployment efforts. For each transit AS, we took the mean AS hegemony score considering paths to all valid announcements and then the score considering paths to all invalid announcements. Of 163 ASes that propagated both valid and invalid announcements, 11 had a larger mean hegemony score for invalid announcements, suggesting that those ASes were more likely to propagate invalid announcements. Those 11 ASes could also serve as a starting point for improved future ROV deployment. (Note there is no overlap with detour ASes, who propagate *only* invalids.)

5 LIMITATIONS AND FUTURE WORK.

Justifiable propagation of invalids. We found a case where AS2914 (NTT, which rigorously performs ROV) propagated 2 invalid announcements originated by a test AS for RPKI experiments. To filter such possible situations as such, we analyzed only ASes propagating > 2 invalid announcements. Navigating special operational cases is important future work.

Limitations of public BGP data We only had access to public BGP datasets which have an incomplete view of the global routing table. Our methodology could be used in combination with less public and/or more complete data sources to improve visibility of propagation of RPKI invalid announcements.

Inability to simulate changes. We are cautious about assuming that new ROV deployment will prevent propagation of invalids. As we have seen, invalid announcements may find new paths (or unobserved existing backup paths) to reach corners of the Internet.

ACKNOWLEDGMENTS

This work is based on research sponsored by U.S. NSF grants OAC-2131987 and CNS-2120399. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of NSF.

REFERENCES

[1] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Roland van Rijswijk-Deij, John Rula, and Nick Sullivan. 2019. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet Measurement Conference* (Amsterdam, Netherlands) *(IMC '19)*. Association for Computing Machinery, New York, NY, USA, 406–419.

[2] Ben Du, Gautam Akiwate, Thomas Krenc, Cecilia Testart, Alexander Marder, Bradley Huffaker, Alex C Snoeren, and KC Claffy. 2022. IRR Hygiene in the RPKI Era. In *International Conference on Passive and Active Network Measurement*. Springer, 321–337.

[3] Ben Du, Cecilia Testart, Romain Fontugne, Gautam Akiwate, Alex C. Snoeren, and kc claffy. 2022. Mind Your MANRS: Measuring the MANRS Ecosystem. In *Proceedings of the 22nd ACM Internet Measurement Conference* (Nice, France) *(IMC '22)*. Association for Computing Machinery, New York, NY, USA, 716–729.

[4] Romain Fontugne, Anant Shah, and Emile Aben. 2018. The (thin) bridges of as connectivity: Measuring dependency using as hegemony. In *International Conference on Passive and Active Network Measurement*. Springer, 216–227.

[5] Geoff Huston and Joao Damas. 2020. Measuring Route Origin Validation. https://www.potaroo.net/ispcol/2020-06/rov.html

[6] Internet Initiative Japan. 2023. Internet Health Report. ttps://ihr.iijlab.net/ihr/en-us/rov

[7] Kevin Klercq, Willem Toorop, and Koen van Hove. 2023. ImpROVement. RIPE 86. https://ripe86.ripe.net/wp-content/uploads/presentations/144-ImpROVement.pdf

[8] Cecilia Testart, Philipp Richter, Alistair King, Alberto Dainotti, and David Clark. 2020. To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today. In *International Conference on Passive and Active Network Measurement*. Springer, 71–87.