Taking the Low Road: How RPKI Invalids Propagate

Ben Du[1] Cecilia Testart[2] Romain Fontugne[3] Alex C. Snoeren[1] KC Claffy[1]

[1]UC San Diego [2]Georgia Tech [3]IIJ Research Labs

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.

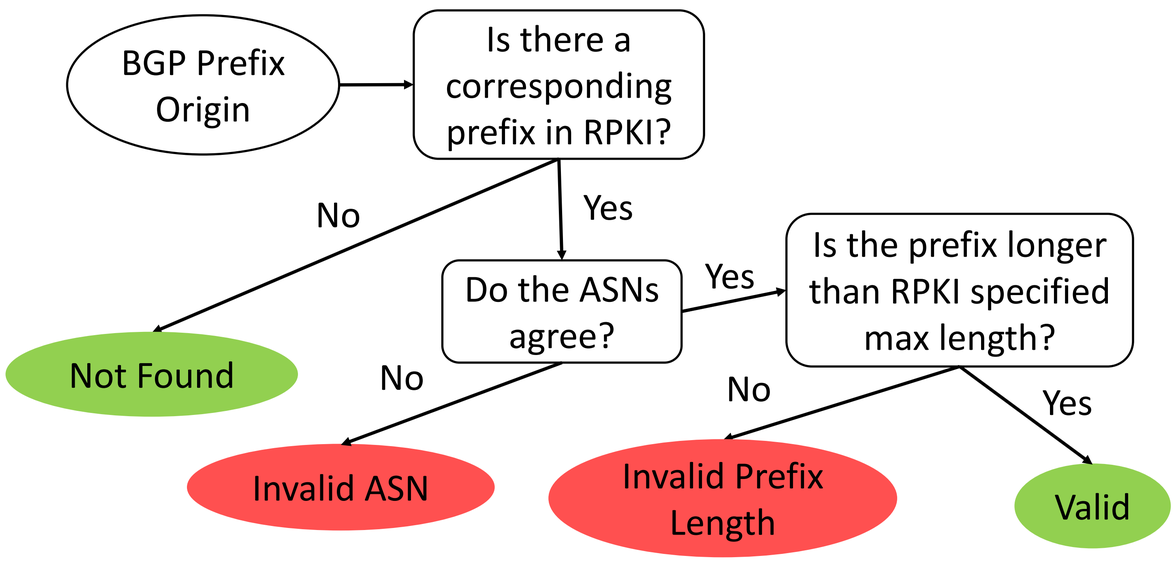
Problem

Operational and legal constraints have prevented full RPKI deployment, so malicious or misconfigured routing information can still propagate across the Internet.

- Only a subset of networks have registered in the RPKI.
- Fewer networks use RPKI-based route filters.

Background

RFC 6811 uses RPKI to classify each BGP announcements as follow. Networks should filter Invalid ASN or Invalid Prefix Length.

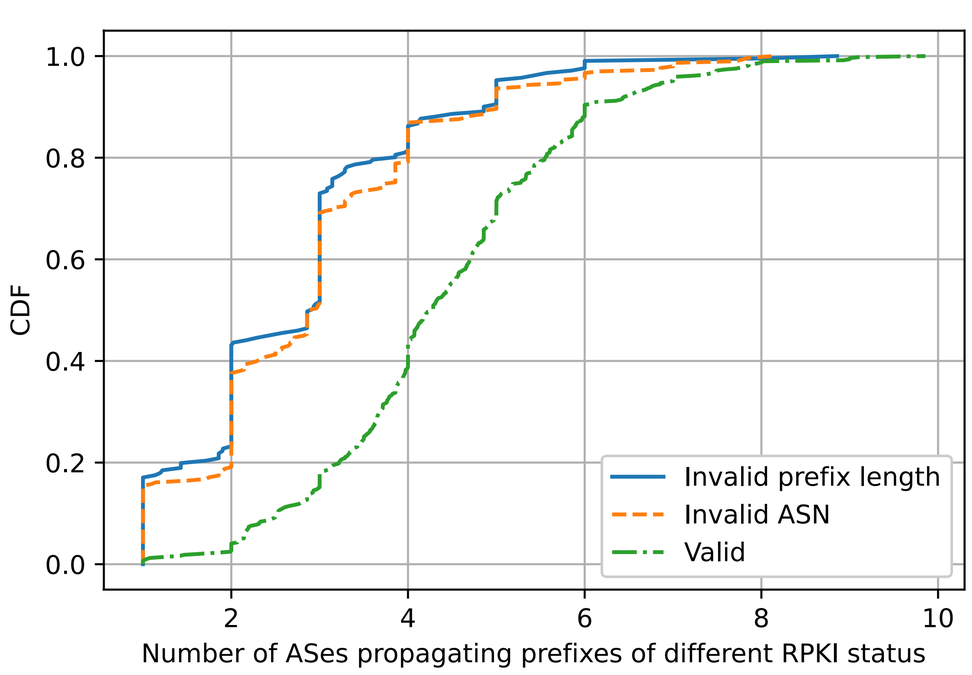


Research Questions

RQ1: How far across the internet do RPKI-invalids propagate?
RQ2: How do RPKI-invalid announcements propagate?
RQ3: Which detour ASes propagate the most RPKI-invalids?

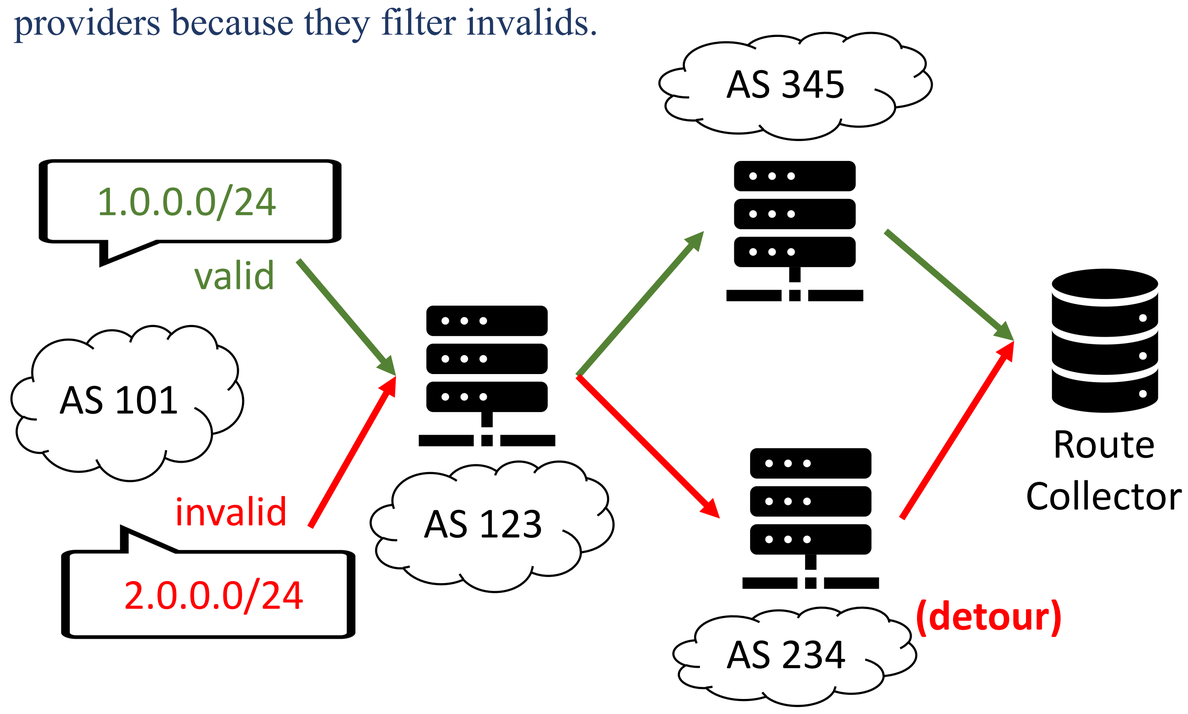
RQ1- RPKI-invalid announcements propagate less farther across the Internet

- We found that RPKI-valid announcements had more transit ASes than RPKI-invalid announcements (See figure below).
- The 40th percentile of RPKI-invalid announcements propagated across 2 ASes while RPKI-valid announcements propagated across 4 ASes.
- Enough ASes have now deployed ROV to cause a topological difference between the propagation of RPKI-valid and invalid announcements.



RQ2 – RPKI-invalid announcements detour around primary transit ASes

We can examine how invalid announcements propagate by focusing on ASes that originate both valid and invalid prefixes. In particular, invalid announcements may take a **detour** around the origin AS' primary transit providers because they filter invalids.



RQ3- 115 ASes appeared as backup transit for RPKI-invalid announcements

We consider a transit AS detour if it propagated only RPKI-invalid announcements for at least one origin AS.

- 115 (25%) out of 457 unique ASes that propagated RPKI-invalid announcements were detour ASes.
- 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.

The table below shows the top 10 detour ASes that propagated RPKI-invalid announcements from the most origin ASes.

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

Summary

We identified ASes that propagate RPKI invalid prefixes. If the ASes responsible for propagating the most invalid prefixes were to deploy ROV, it could dramatically increase the security of the routing ecosystem.

Challenges and Future Work

Experimental invalid announcements: Some invalids are from network experiments. Navigating special operational cases is important future work.

Dynamic network topology: Invalid announcements may find new paths (or unobserved existing backup paths) to reach corners of the Internet.

Acknowledgements: This work is based on research sponsored by U.S. NSF grants OAC2131987 and CNS-2120399. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of NSF.