Measuring Route Origin Validation

Setting up a useful RPKI Beacon

Willem Toorop
20 March 2022
IEPG at IETF113 Vienna
Why this presentation

- I had to setup an RPKI Beacon, but I’m not an RPKI expert
- I need your opinion – does what I did make sense
- I need your brains – how to best measure ROV?
- I want the beacon to be usable (available) for you too!
- We could also use some additional IPv4 resources 😄
Genesis

- I do DNS measurements (with RIPE Atlas mostly)
- Job Snijders offered to use his RPKI Beacon during IMC2019 in Amsterdam 😊💖
- Started measuring the uptake Of Route Origin Validation since Januari 2020
- Job’s beacon EOL in Oct. 2020
The Current State of DNS Resolvers and RPKI Protection

Marius Brouwer
University of Amsterdam
marius.brouwer@uva.nl

Erik Dekker
University of Amsterdam
erik.dekker@uva.nl

ABSTRACT
The goal of this research was to gain insight into the Resource Public Key Infrastructure (RPKI) protection state of DNS resolvers. RIPE Atlas Probes were used to send DNS queries to an authoritative DNS server. This server contained Resource Records in both an RPKI valid and invalid prefix. The RIPE Atlas probes were instructed to send these requests to different resolvers.

The resolvers demonstrated varying levels of RPKI awareness. The DNSSEC support of some resolvers was also tested.

Due to the distributed nature of BGP and RPKI, the majority of network operators should sign their network prefixes and implement RPKI filtering to minimize prefix hijacks and route leaks [9].

A study conducted in 2019 claimed that between 9.98% and 11.28% of the BGP announcements were verifiable using RPKI [10].

security, it is not broadly adopted [7, 8]. For this reason, this paper will focus on RPKI.

AS21 drops RPKI invalid BGP routes from prefix 2001:67c:64:ae5b00:0129:eb9c:65c

testing valid ROA...[passed]
testing invalid ROA (5sec)...[passed]

100% 3 check(s)
100% 3 check(s)
100% 2 check(s)

Achievements
Re-evaluate setup - before

  - ✔ If endpoint validates → invalid = unreachable
  - ✗ If any hop in between validates → invalid = unreachable
  - ✗ Validating hop may be in return path
Re-evaluate setup - before
Re-evaluate setup - before

  
  ✔ If endpoint validates → invalid = unreachable
  ❌ If any hop in between validates → invalid = unreachable
  ❌ Validating hop may be in return path

  ❌ Is this a realistic route hijack?
  ❌ Unreachable detection based on timeout
Re-evaluate setup - new setup

- Valid /23 (IPv4) and /47 (IPv6) and Invalid /24 and /48 more specific announcements from elsewhere
  - ✔ More realistic route hijack?
  - ✔ Don’t have to wait for timeouts!
Re-evaluate setup - new setup

- Valid /23 (IPv4) and /47 (IPv6) and Invalid /24 and /48
- More specific announcements from elsewhere
Re-evaluate setup - new setup

- Valid /23 (IPv4) and /47 (IPv6) and Invalid /24 and /48 more specific announcements from elsewhere
  - More realistic route hijack?
  - Don’t have to wait for timeouts!

- Still can’t determine which hop is validating
- Even when your network is validating, you can still reach the invalid!
Re-evaluate setup - new setup

- Valid /23 (IPv4) and /47 (IPv6) and Invalid /24 and /48
- More specific announcements from elsewhere
  ✔ More realistic route hijack?
  ✔ Don’t have to wait for timeouts!
  ✗ Still can’t determine which hop is validating
  ✗ Even when your network is validating, you can still reach the invalid!

Picture from the Maelstrom Ascendant book and album.
Copyright by: Duncan Smith
Re-evaluate setup - new setup
Apps

- CMDNS: Moved 👍
- Resolver test: Very fast! 👍
- RPKI NCC
  Web test: Ont it's way 👍
For you!

@ RIPE Atlas
For you! 🎁

@ RIPE Atlas

@ NLNOG Ring
For you! 🎁

@ RIPE Atlas

@ NLNOG Ring
For you! 🎁

@ RIPE Atlas

@ NLNOG Ring

Measure services

Should they?

@ Anything else?
Why - questions & feedback

● I need your opinion – does what I did make sense?
● I need your brains – how to best measure ROV?
● I want the beacon to be usable (available) for you too! – what tool do you want/need?
● We could also use some additional IPv4 resources – Collaborate?