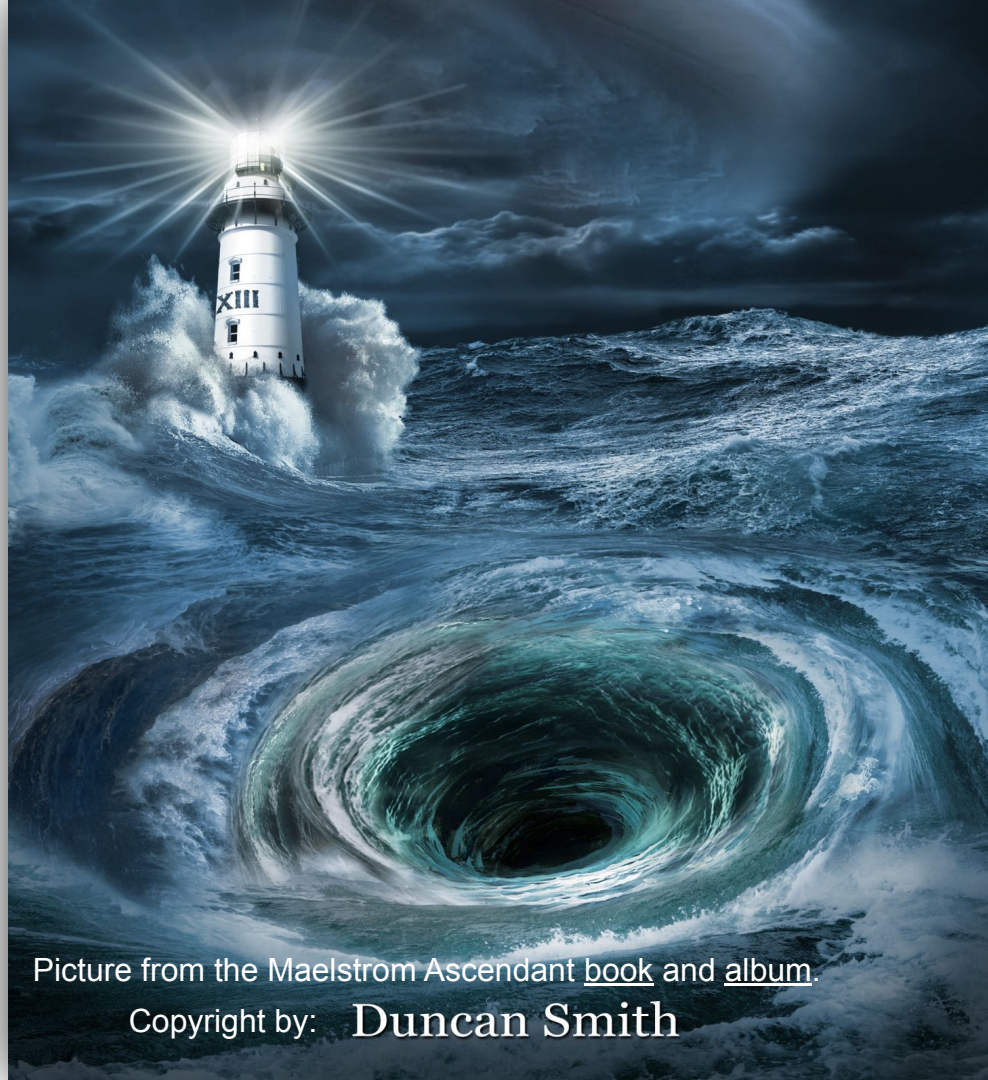# Measuring Route Origin Validation

Setting up a useful RPKI Beacon

Willem Toorop
20 March 2022
IEPG at IETF113 Vienna

Picture from the Maelstrom Ascendant book and album.
Copyright by: Duncan Smith

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

RPKI TEST a RIPE Labs experiment

testing valid ROA...[passed]
testing invalid ROA (5sec)...[passed]
AS2121 drops RPKI invalid BGP routes from prefix 2001:67c:64::/48 as witnessed by your public IP 2001:67c:64:42:84ae:5b00:a129:e85c
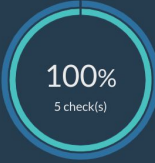
Check My DNS – Chromium

Check My DNS
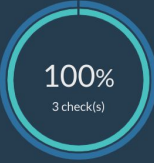
cmdns.dev.dns-oarc.net

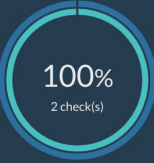# Check My DNS A

Transport — 100% — 5 check(s)
Basic DNS — 100% — 3 check(s)
DNS Features — 100% — 2 check(s)

Achievements

Cli IPv6   RPKIv4   RPKIv6

© 2021 OARC, Inc.   Feedback @ GitHub / @dnsoarc / email

Probe/resolver pairs

Remaining
Init Seven AG
Hurricane Electric, Inc.
Societe Francaise du Radiot... ...S.A
Versatel Deutschland Gm...
XS4ALL Internet BV
Comcast Cable Communica...
VeriSign Infrastructure & ...ions
Free SAS
CloudFlare, Inc.

53
DNSThought
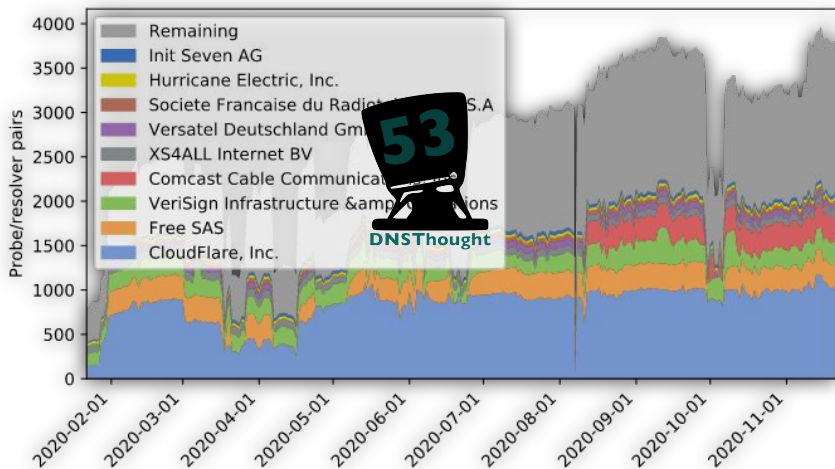
The Current State of DNS Resolvers and RPKI Protection

Marius Brouwer
University of Amsterdam
marius.brouwer@os3.nl

Erik Dekker
University of Amsterdam
erik.dekker@os3.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 their queries

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

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 claims that between 9.98% and 11.28% of the BGP announcements are verifiable using RPKI [10].

Re-evaluate setup - before

● Invalid IPv4 /24 & IPv6 /48 + /24 & /48 valids for reference

✔ If endpoint validates → invalid = unreachable

✗ If any hop in between validates → invalid = unreachable

✗ Validating hop may be in return path

Re-evaluate setup - before
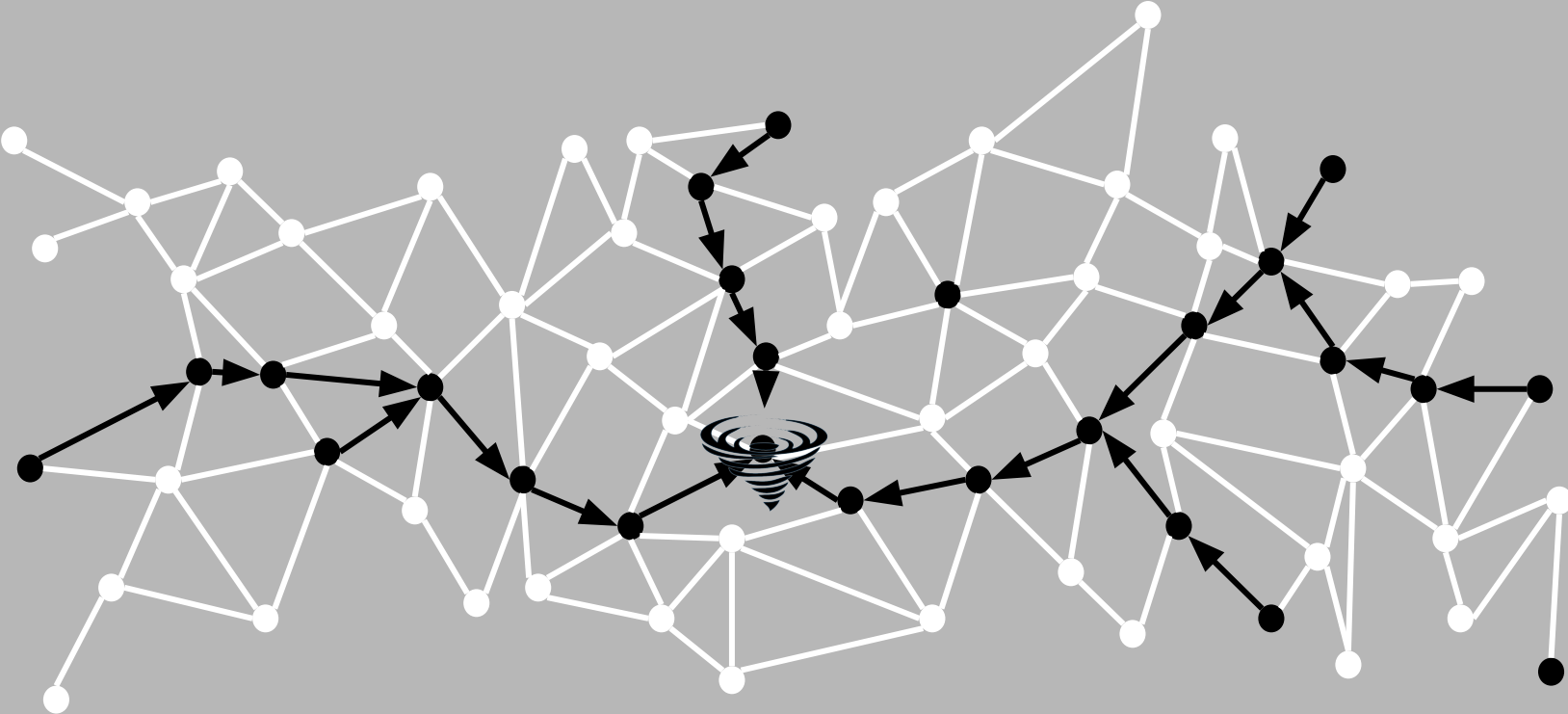
Re-evaluate setup - before

- Invalid IPv4 /24 & IPv6 /48 + /24 & /48 valids for reference

    ✔ 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-e

- Vali[...]   48
  mor[...]

Krill - RPKI - Chromium

Krill - RPKI

prod-ca.krill.cloud/index.html#/cas/nlnetlabs

Krill

English

Certificate Authority **nlnetlabs**

ROAs   Parents   Repository

185.49.142.0

Download CSV

ASN	Prefix	State	
0	185.49.142.0/24-24	REDUNDANT	🗑
14618	185.49.142.0/23-23	DISALLOWING 1	🗑
16509	185.49.142.0/23-23	SEEN 1 1	🗑
211321	185.49.142.0/24	INVALID ASN	+

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-evalu...

- Valid /23 (... and /48 more spe...
  - ✔ More r...
  - ✔ Don't h...

  - ✗ Still ca...g
  - ✗ Even w...
    you ca...
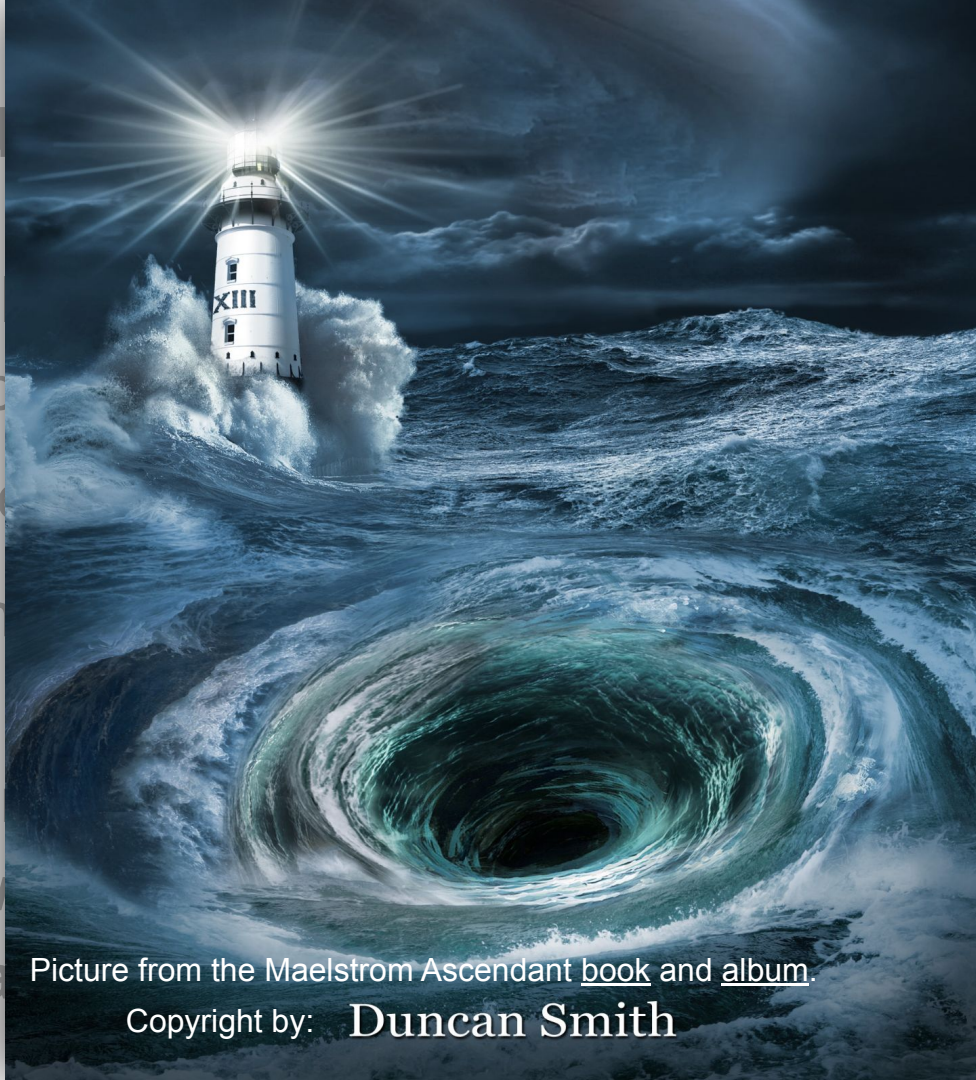
Picture from the Maelstrom Ascendant book and album.
Copyright by: Duncan Smith

Re-evaluate setup - new setup
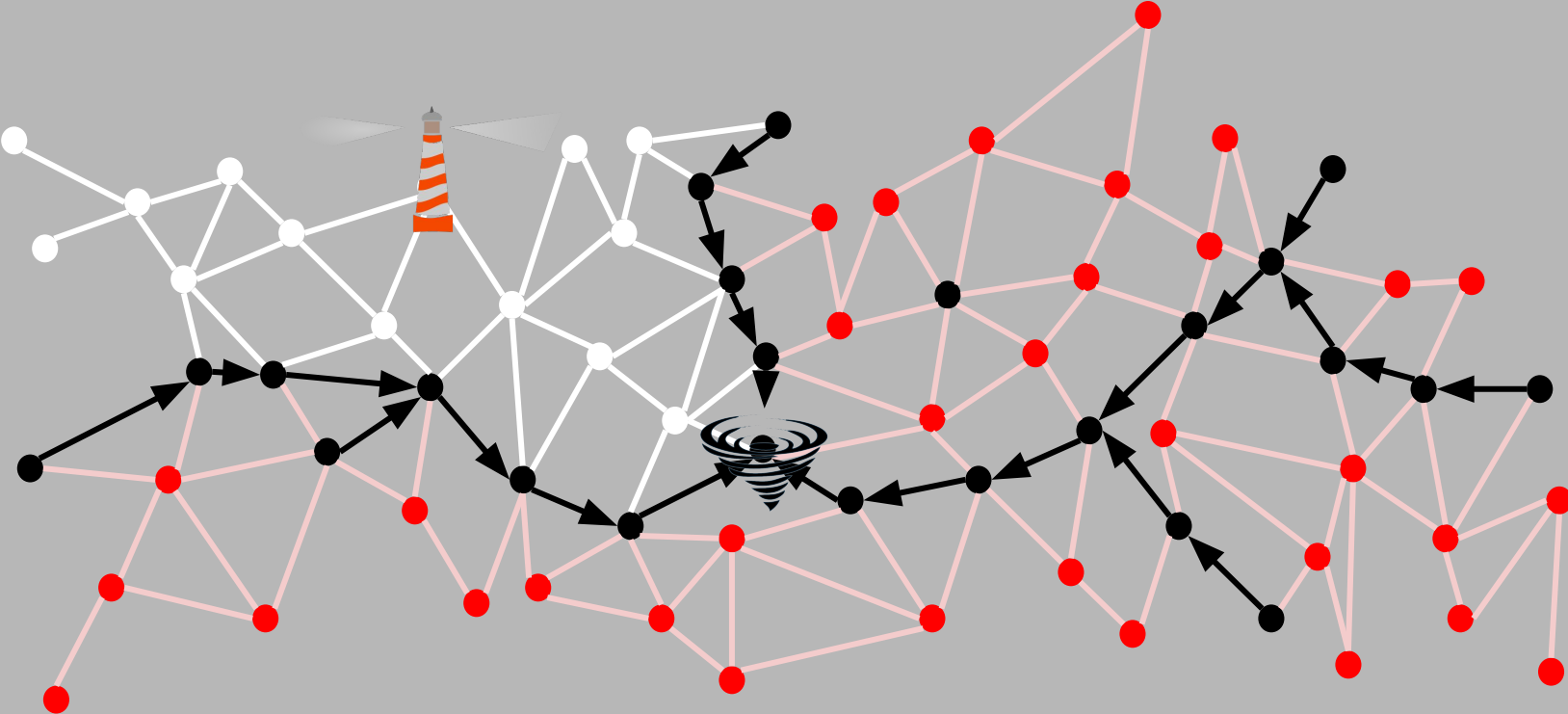
Apps

- CMDNS:
  Moved 👍

- Resolver test:
  Very fast! 👍

- RPKI NCC
  Web test:
  Ont it's way 👍


```
willem@makaak:~$ dig @1.1.1.1 rpkitest4.nlnetlabs.nl TXT

; <<>> DiG 9.16.15-Ubuntu <<>> @1.1.1.1 rpkitest4.nlnetlabs.nl TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36209
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;rpkitest4.nlnetlabs.nl.                    IN      TXT

;; ANSWER SECTION:
rpkitest4.nlnetlabs.nl. 1          IN      TXT     "HOORAY - Your resolver is prote
cted by Route Origin Validation :)!"

;; Query time: 32 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: do mrt 17 15:41:43 CET 2022
;; MSG SIZE  rcvd: 130

willem@makaak:~$
```

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?**