Where did my packet go?
Measuring the impact of RPKI ROV

Koen van Hove

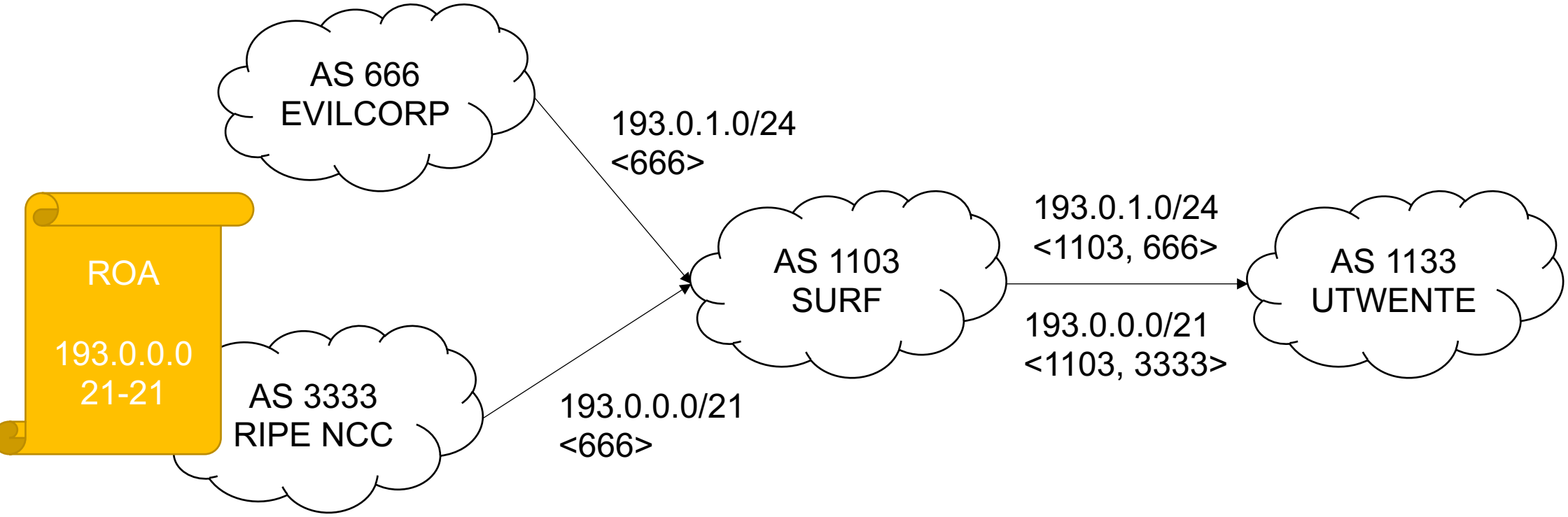
IEPG at IETF 114

Why do we care about RPKI?

- We care where the traffic actually goes to …
- … and whether we intended the traffic to end up there

What is the problem?

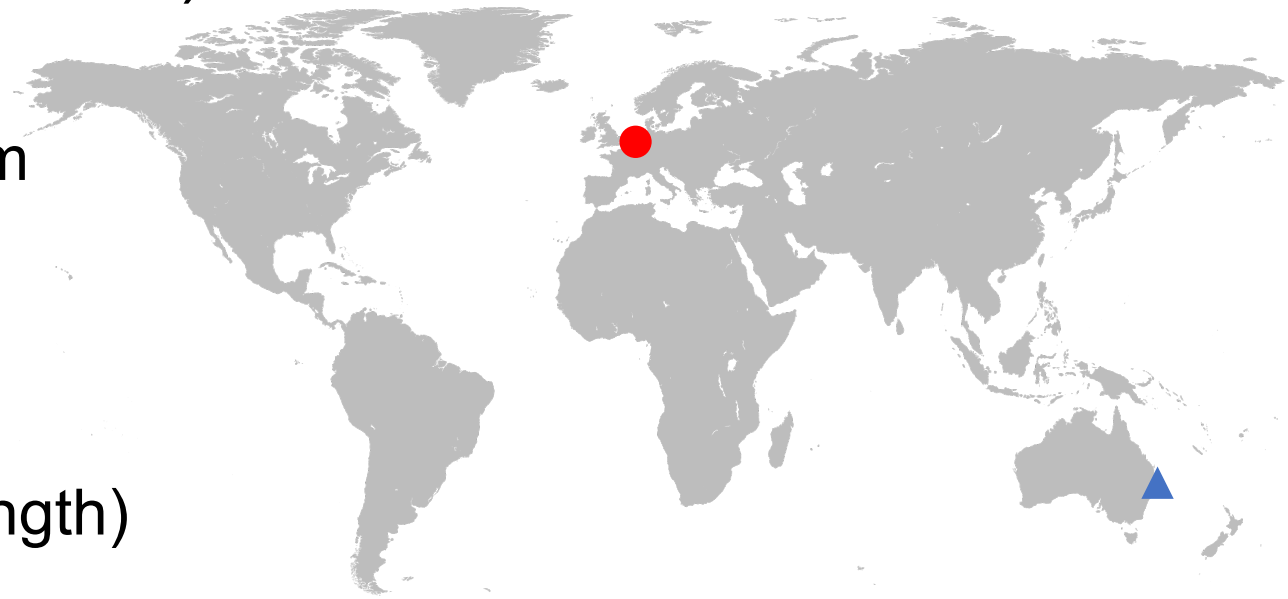
- We have limited control over where our upstream sends the traffic to



The experiment (1)

- One AS – AS 211321 (NLnet Labs)
- Two servers
  - ● One at ColoClue in Amsterdam
  - ▲ One at Vultr in Sydney
- Some announced prefixes
  - ▲ 2a04:b905::/32 (valid)
  - ● 2a04:b905::/33 (invalid maxlength)
  - ▲ 2001:ddb::/48 (invalid AS0)

  (and their IPv4 equivalents 203.119.22.0/23, 203.119.22.0/24, 203.119.21.0/24)



The experiment (2)

- Three RPKI publication points:
  - parent.rov.koenvanhove.nl (2a04:b905:8000::1)
  - child.rov.koenvanhove.nl (2a04:b905::2)
  - invalid.rov.koenvanhove.nl (2001:ddb::1)
- If everyone does ROV, then the traffic for child.rov.koenvanhove.nl will end up at Vultr (less specific and valid).
- If they do not, traffic will go to ColoClue (more specific and invalid)
- invalid.rov.koenvanhove.nl to determine whether organisation does ROV and drops invalids (no other route available)

Why RPKI publication points?

- Every measurement has a bias
- More likely to do ROV than the average

Results

Results of where traffic ended up based on whether they did ROV and dropped invalids per unique IP address

	Ends up at ColoClue in Amsterdam (invalid)	Ends up at Vultr in Sydney (valid)
Drops invalids	304	1650
Does not drop invalids	600	628

Challenges (1)

- At first, 99% of traffic went to ColoClue ...
- … Vultr did not do ROV …
- … traffic would reach the Vultr edge and get redirected to another tier 1 …
- … and end up in Amsterdam

- Solved by also announcing the more specific at Vultr with a BGP community that prevents export outside Vultr

Challenges (2)

- Our ROA was only hosted on parent.rov.koenvanhove.nl
- Initially that was IPv6-only (getting IPv4 is difficult)
- Not all networks that handle IPv6 traffic actually support IPv6 where their validators run
- This even triggered internal alerts due to mismatches for some organisations

Conclusion

- Merely doing ROV (and dropping invalids) does not mean your traffic goes to the intended location
- The more varied your upstreams are, the more important doing ROV is
- Live map of data coming in on https://rov.koenvanhove.nl
- Article on RIPE Labs: https://labs.ripe.net/author/koen-van-hove/where-did-my-packet-go-measuring-the-impact-of-rpki-rov/

- Thank you NLnet Labs and RIPE NCC for letting me do BGP things using your resources :-)