Secure BGP routing vs. reality

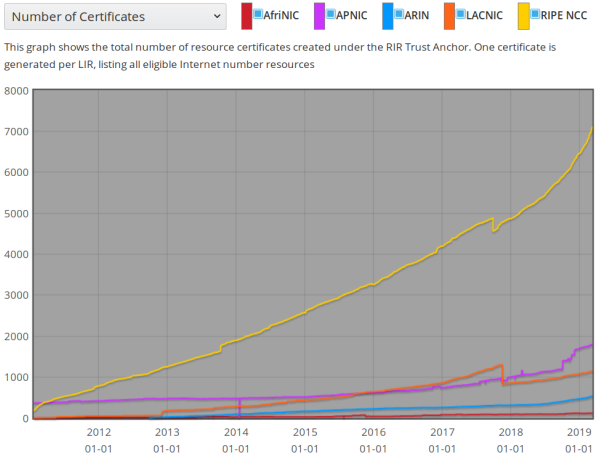
Tomáš Hlaváček (tomas.hlavacek@nic.cz)

Tuesday 12th March, 2019 • CEE Peering Days 2019, Zagreb

RPKI

- Resource Public Key Infrastructure
- Makes Internet routing more secure
- Opt-in
- Route Origin Authorizations (ROAs)
- Route Origin Validation (ROV)
- Hosted RPKI - by RIRs

ROA stats



Source: http://certification-stats.ripe.net

ROV

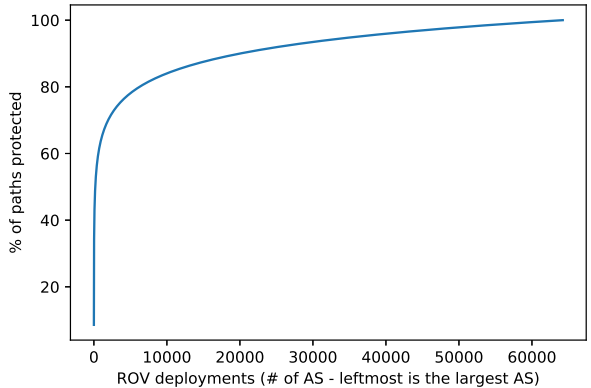
- Route Origin Validation
- Possible results are: Valid, Not-found, Invalid
- What to do with Invalid? Validating host/network decides: De-prefer? Drop? Pass?

But ROV is seldom enforced:

- Experiments (presented here two years ago) indicate that only about 0.1% of ASNs in the Internet enforced ROV validation.
- Only 2 (verified) and 12 (likely) out of 2106 ASNs enforce ROV!
- Independent experiment - *Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering* by A. Reuter, R. Bush, I. Cunha, E. Katz-Bassett T. Schmidt and M. Wählisch came to the same overall result.
- Ongoing measurements based on the former methodology: `https://rov.rpki.net/`

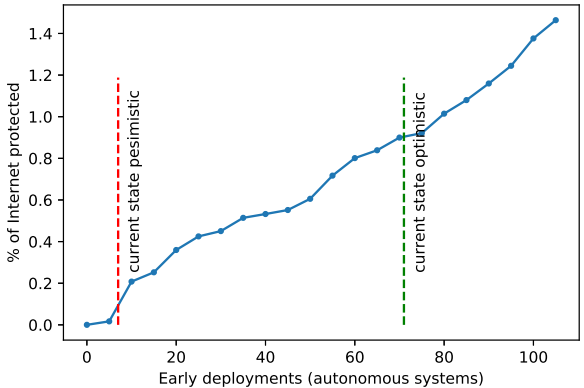
ROV theoretical benefits

- ROV on "Internet backbone" would prevent almost all global hijacks
- ROV in IX would save localized hijacks



ROV benefits in reality (simulation)

- ROV is supported by Route Servers (AMS-IX)
- several AS operators enforce ROV

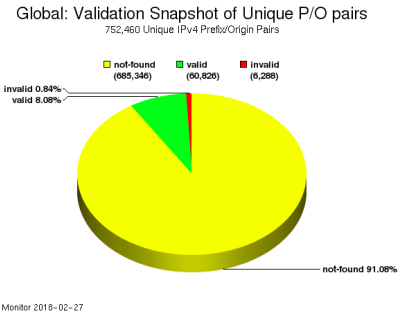


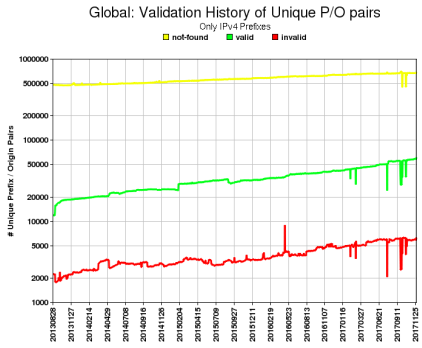
Why not (enough) ROV?

- Concerns about a "new" technology,
- distrust in "complex" system, crypto, ...,
- **concerns about disconnected networks & lost traffic due erroneous ROAs**,
- missing business case for RPKI,
- distrust in the authority transfer to a formal hierarchy that can at some point work against freedom of the Internet.

Concerns about disconnects & lost traffic

- It is easy to find conflicts between ROA origins and origins observed in BGP and ...
- NIST did that for us!
- What do we know about the conflicts?

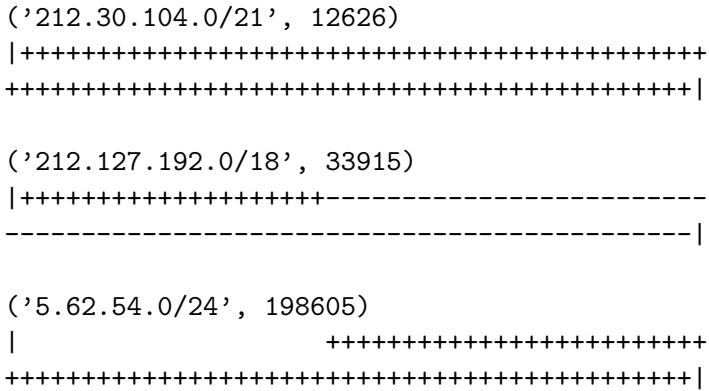




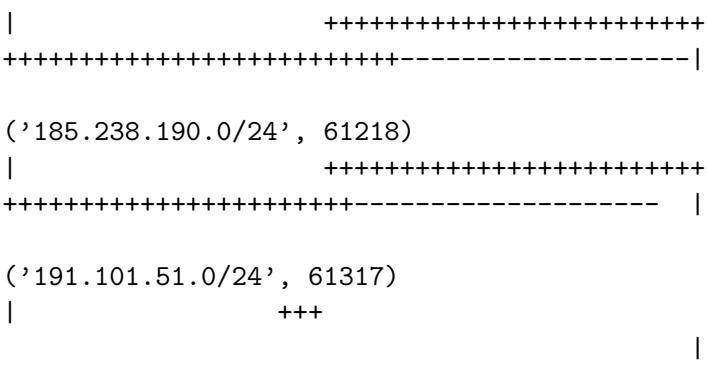
Prefix/Origin RPKI conflicts

- unknown (no relevant ROA):
  - v4: 687032 (87.49%)
  - v6: 58868 (84.33%)
- valid (at least one valid ROA):
  - v4: 93984 (11.97%)
  - v6: 10255 (14.69%)
- invalid ASN:
  - v4: 1089 (0.14%)
  - v6: 101 (0.14%)
- invalid prefix length:
  - v4: 3124 (0.40%)
  - v6: 580 (0.83%)
- timestamp (results valid at): 2019-03-11 16:00:00

Conflict timeline examples



Conflict timeline examples (cont.)



Observations

- Timeline patterns are quite regular
- The patterns even correlate on groups of prefixes and ASNs
- IRR data for the conflicting P/O pairs can be correlated
- Experiments with machine learning for conflict pattern recognition by Fraunhofer SIT researchers shows this could be a viable way of whitelisting forgotten and outdated ROAs
- Several attempts to draw attention of admins to outdated ROAs (e-mail campaigns)
- The conflict remedy time in many cases correlate with the campaign periods

Coming soon...

https://bgpsec.labs.nic.cz/

Thank you!

Questions?