



ROV adoption consequences

Tomáš Hlaváček (tomas.hlavacek@nic.cz)

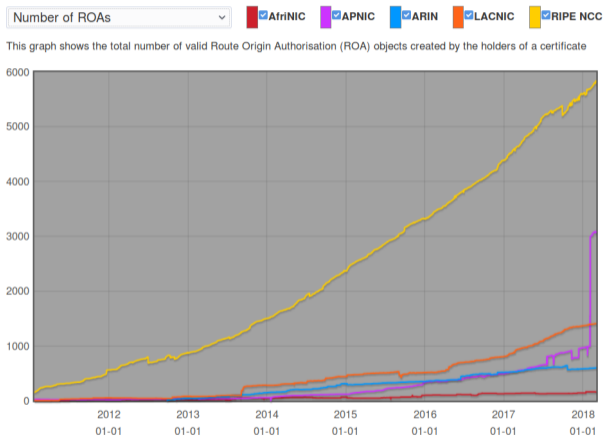
Wednesday 7th March, 2018 • CEE Peering Days 2018, Berlin

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

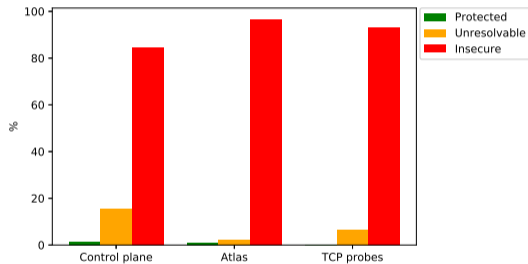
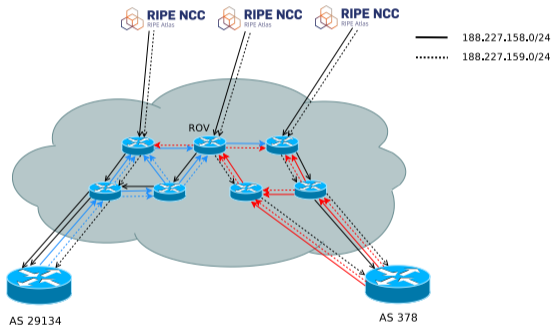
- ▶ Route Origin Validation
- ▶ Possible results are: Valid, Not-found, Invalid
- ▶ What to do with Invalid? Validating host/network decides: De-prefer? Drop? Pass?

But ROV is seldom enforced:

- ▶ Experiments (presented here last year) indicate that only about **0.1% of ASNs in the Internet enforces 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, Í. Cunha, E. Katz-Bassett T. Schmidt and M. Wählisch came to the same overall result.



The ROV Experiment



Why no 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 would be the impact of ROV on traffic?

Global: Validation Snapshot of Unique P/O pairs

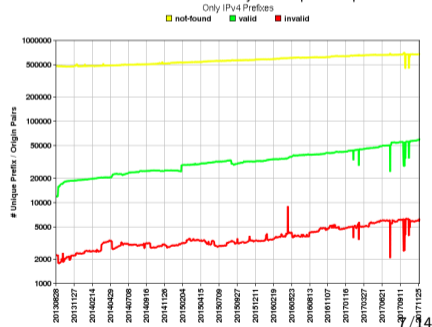
752,460 Unique IPv4 Prefix/Origin Pairs



NIST RPKI Monitor 2018-02-27

Source: <https://rki-monitor.andt.nist.gov/>

Global: Validation History of Unique P/O pairs

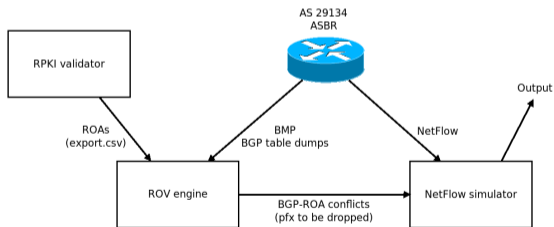


NIST RPKI Monitor 2018-02-27

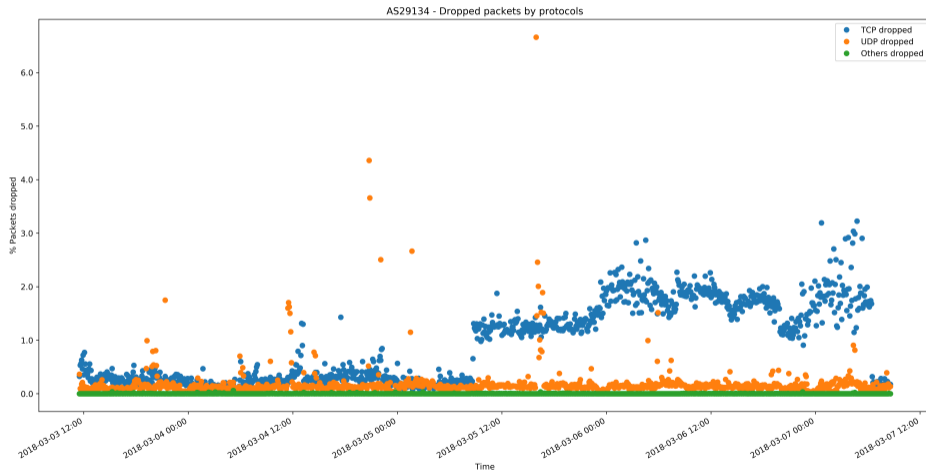
Concerns about disconnects & lost traffic (cont.)

Let's find out how bad is it...

- ▶ ROV impact on traffic can be simulated!
- ▶ Requirements: BGP feed, published ROAs, traffic trace in a suitable format - NetFlow
- ▶ *Thanks for AS29134 (Igunum, s.r.o.) for providing them!*



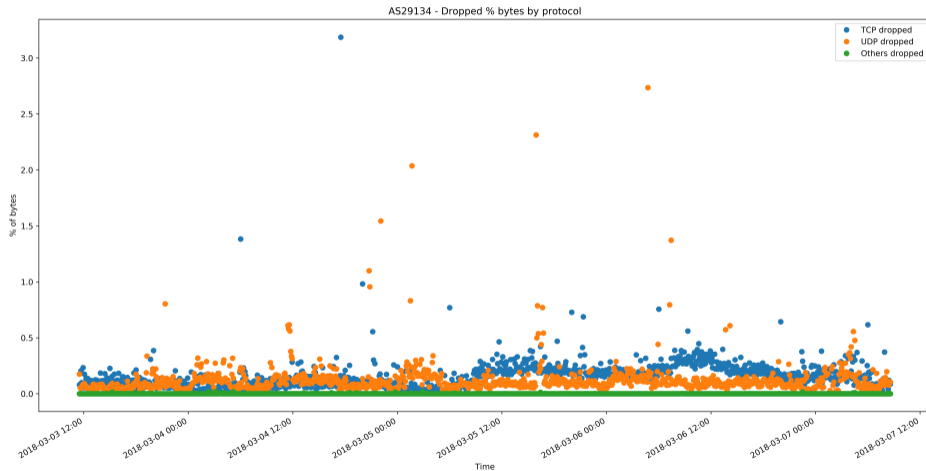
Results



9/14



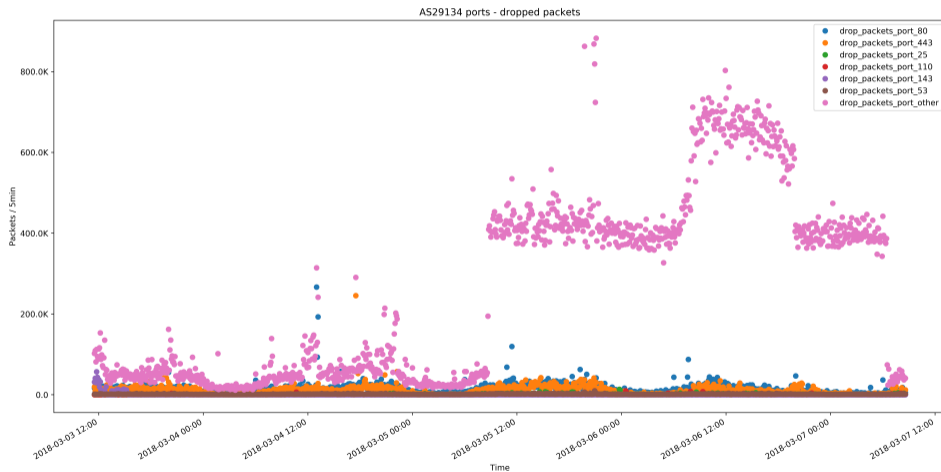
Results (cont.)



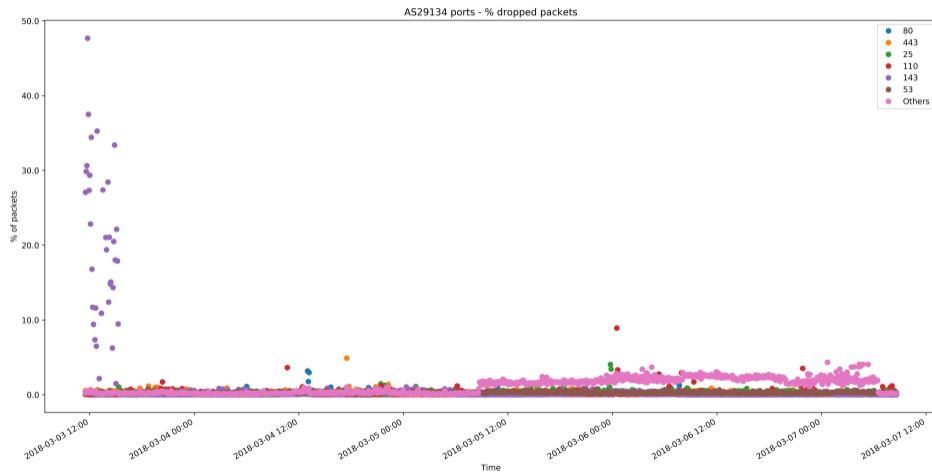
10/14



Results (cont.)



Results (cont.)



12/14



Why no ROV? (again)

- ▶ ~~Concerns about a "new" technology:~~
 - ▶ RIPE NCC RPKI Validator, developed since 2011, currently version 2.24,
 - ▶ router support: IOS-XE 3.5.0, IOS 15.1(3)S, IOS-XR 4.2.1, JunOS since 12.2R1,
 - ▶ proven in the wild: AS8283, AS50300 and AS59715,
- ▶ ~~distrust in "complex" system, crypto, ...:~~ Definitely not as bad as HTTP/HTTPS and BGP,
- ▶ **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.



What's next?

- ▶ Integrate ROV simulator with IDS - distinguish and quantify legitimate traffic from attacks within the filtered packets,
- ▶ invite more networks to participate in our study,
- ▶ answer the question what would happen when ROV is switched on in a particular network
- ▶ and describe global benefits & downsides of ROV.



Thank you!

Questions?

