Simulace dopadů nasazení validace RPKI (ROV)

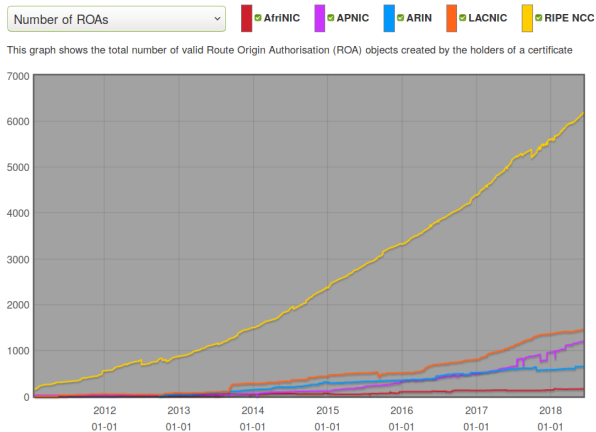
Tomáš Hlaváček (tomas.hlavacek@nic.cz)

12. června 2018 • CSNOG 2018

RPKI

- Resource Public Key Infrastructure
- Cíl: Zabezpečit směrování v Internetu
- Opt-in
- Route Origin Authorizations (ROA)
- Route Origin Validation (ROV)
- Hostované RPKI - implementovaly RIR (RIPE, ...)

Statistiky ROA

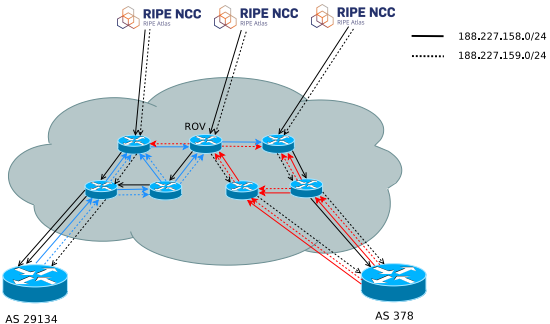


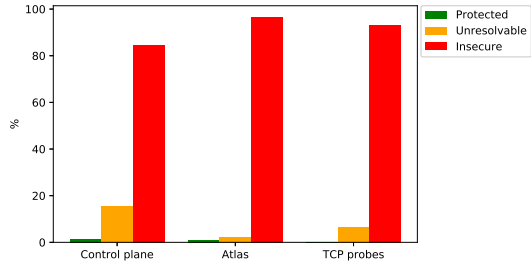
Zdroj: http://certification-stats.ripe.net

ROV

- Route Origin Validation
- Možné výsledky validace: Valid, Not-found, Invalid
- Co udělat s Invalid?: Rozhoduje každý ISP, který implementuje ROV.
- Možnosti: Snížit preferenci? Zahodit? Propustit?

Experiment na vyhledání ROV





Experiment na vyhledání ROV

ROV se nicméně uplatňuje zřídka (2016/2017):

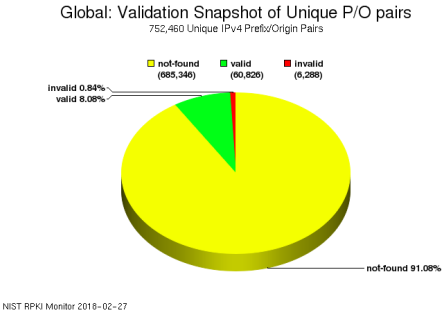
- Experimenty ukázaly že pouze 0.1% autonomínch systémů v Internetu validují a využívají výsledky ROV k ovlivnění routingu.
- Pouze 2 (ověřeno) a 12 (možná) AS aplikují výsledky ROV na routing!
- Nezávislý experiment - *Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering*, autoři A. Reuter, R. Bush, Í. Cunha, E. Katz-Bassett T. Schmidt a M. Wählisch došli k prakticky shodnému výsledku.
- On-line pokračující měření `https://rov.rpki.net/`

Co vadí na ROV?

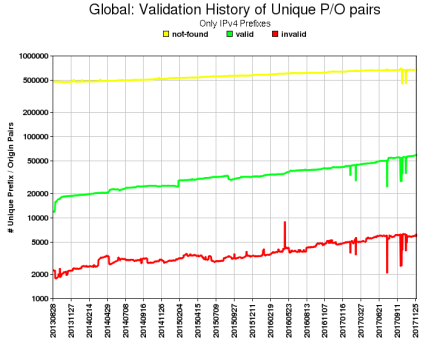
- Obavy z "nové" technologie,
- nedůvěra v "komplexní" systém, krypto, ...,
- **obavy z odpojení vzdálených sítí a ztráty části provozu kvůli chybným ROA**,
- chybějící business case pro RPKI,
- nedůvěra v přenos authority do formální hierarchie, která může narušit svobodu Internetu.

Obavy z odpojení vzdálených sítí a ztráty části provozu

- Konflikty mezi ROA originy and originy v BGP je snadné spočítat ...
- NIST tuto analýzu provedl a zveřejnil na webu.
- Jaký by byl dopad nasazení ROV na provoz?



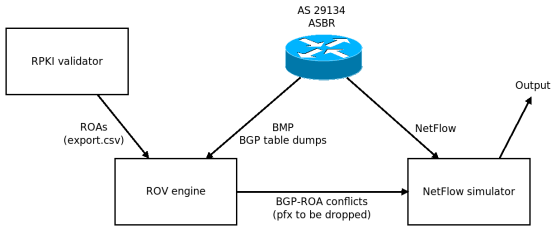
Zdroj: https://rpki-monitor.antd.nist.gov/



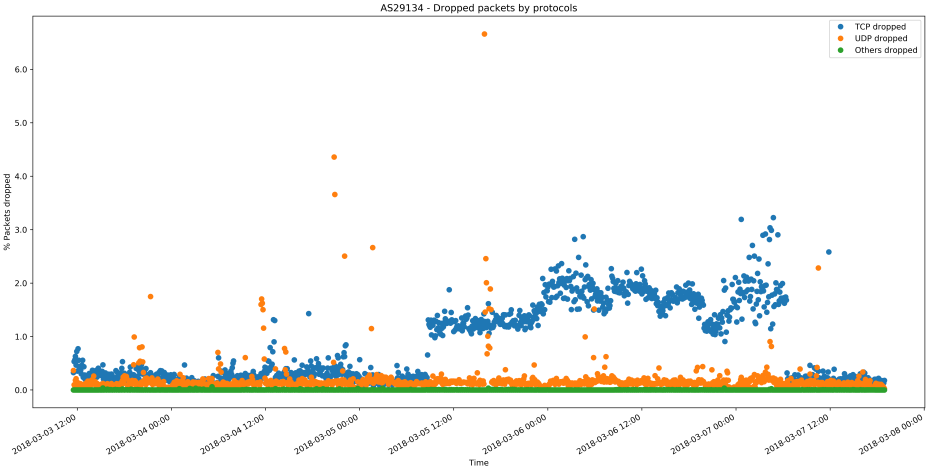
Obavy z odpojení vzdálených sítí a ztráty části trafficu (pokrač.)

Jak prozkoumat dopady nasazení ROV...

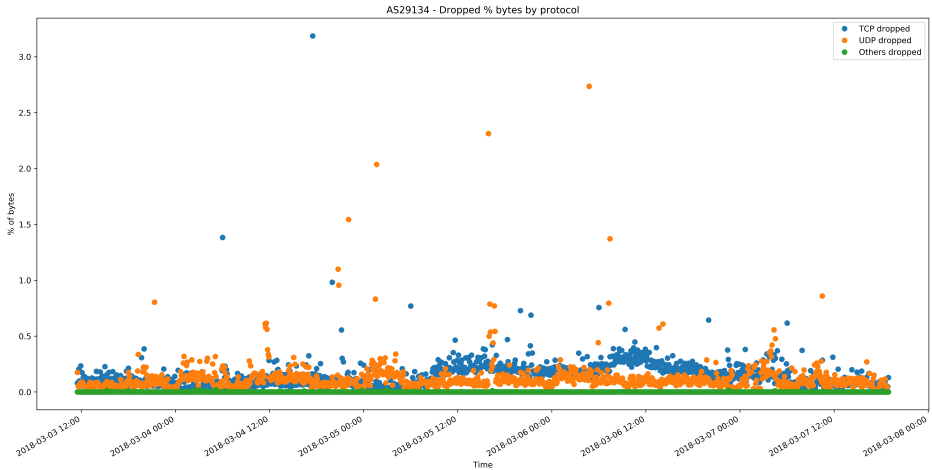
- Lze je simulovat!
- Co je potřeba?: BGP feed, platné publikované ROA, záznam provozu v použitelném formátu - NetFlow
- *Díky AS29134 (Ignum, s.r.o.) za poskytnutí potřebných dat!*



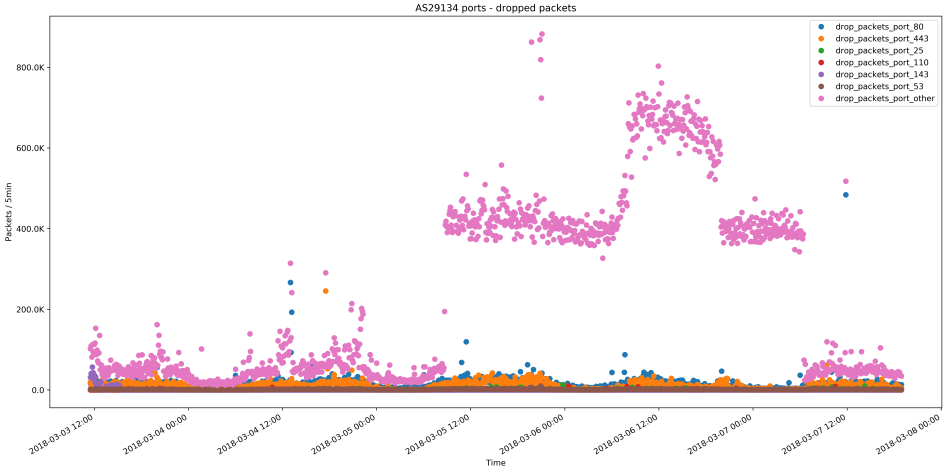
Results



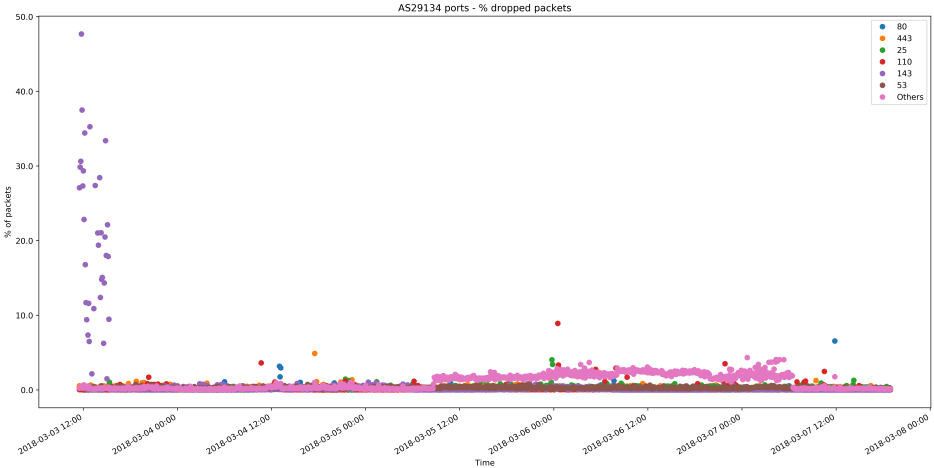
Results (cont.)



Results (cont.)



Results (cont.)



Co vadí na ROV?

- ~~Obavy z "nové" technologie~~:
  - RIPE NCC RPKI Validator, je vyvíjen od roku 2011, současná verze 2.24,
  - podpora routerech: IOS-XE 3.5.0, IOS 15.1(3)S, IOS-XR 4.2.1, JunOS since 12.2R1,
  - reálná nasazení v Internetu: AS8283, AS50300 and AS59715,
- ~~nedůvěra v "komplexní" systém, krypto, ...~~: Ale pořád to není tak zlé, jako HTTP/HTTPS a nebo BGP,
- **obavy z odpojení vzdálených sítí a ztráty části provozu kvůli chybným ROA**,
- chybějící business case pro RPKI,
- nedůvěra v přenos authority do formální hierarchie, která může narušit svobodu Internetu.

Co dál?

- Integrace ROV simulátoru s IDS - automatické rozpoznání a kvantifikace legitimního provozu od útoků v datech, která by byla odfiltrována ROV,
- rozšířit studii o další (větší) sítě,
- odpovědět účastníkům studie otázku, jaký dopad by mělo ROV na jejich síť
- a popsat globální benefity a nevýhody nasazení ROV.

Děkuji za pozornost!

Dotazy?

tomas.hlavacek@nic.cz