RPKI Usage and Consistency

John Kristoff <jtk@depaul.edu>

In collaboration with:

Randy Bush <randy@psg.com>
George Michaelson <ggm@apnic.net>
Thomas C. Schmidt <t.schmidt@haw-hamburg.de>
Matthias Wählisch <m.waehlisch@fu-berlin.de>

Outline

- Secure Routing Background
- Overview of RPKI validation
- Measurement design
- Research Questions and Activity
  - RIR differences
  - Cache servers and consistency
  - Network RPKI effects
- Future Work

Routing Tables

```
inet.0: 804546 destinations, 1583181 routes
+ = Active Route, - = Last Active, * = Both

1.0.0.0/24          *[BGP/170]
                       AS path: 64496 13335 I
                          validation-state: valid
                     [BGP/170]
                       AS path: 64497 64500 13335 I
                          validation-state: valid
```

Route Filters and Max Limits

```
prefix-limit {
    maximum 10000;
}
...
policy-statement sanitize-bgp {
    term rfc1918 {
        from {
            prefix-list-filter rfc1918 orlonger;
        }
        then reject;
    }
```

Internet Routing Registry (IRR)

- Routing policy database(s)
- Intended to help automation and troubleshooting
- Of varying completeness and quality

```
route:          140.192.0.0/16
descr:          DePaul University
descr:          1 E Jackson
descr:          Chicago, IL 60604
origin:         AS20130
member-of:      RS-DEPAUL
```

Route Origin Authorization (ROA)

ROA Name: DEPAUL AS20130

Origin AS: **20130**

Validity Period: 02-12-2019 to 02-12-2029

Resources:

2604:95C0::/32

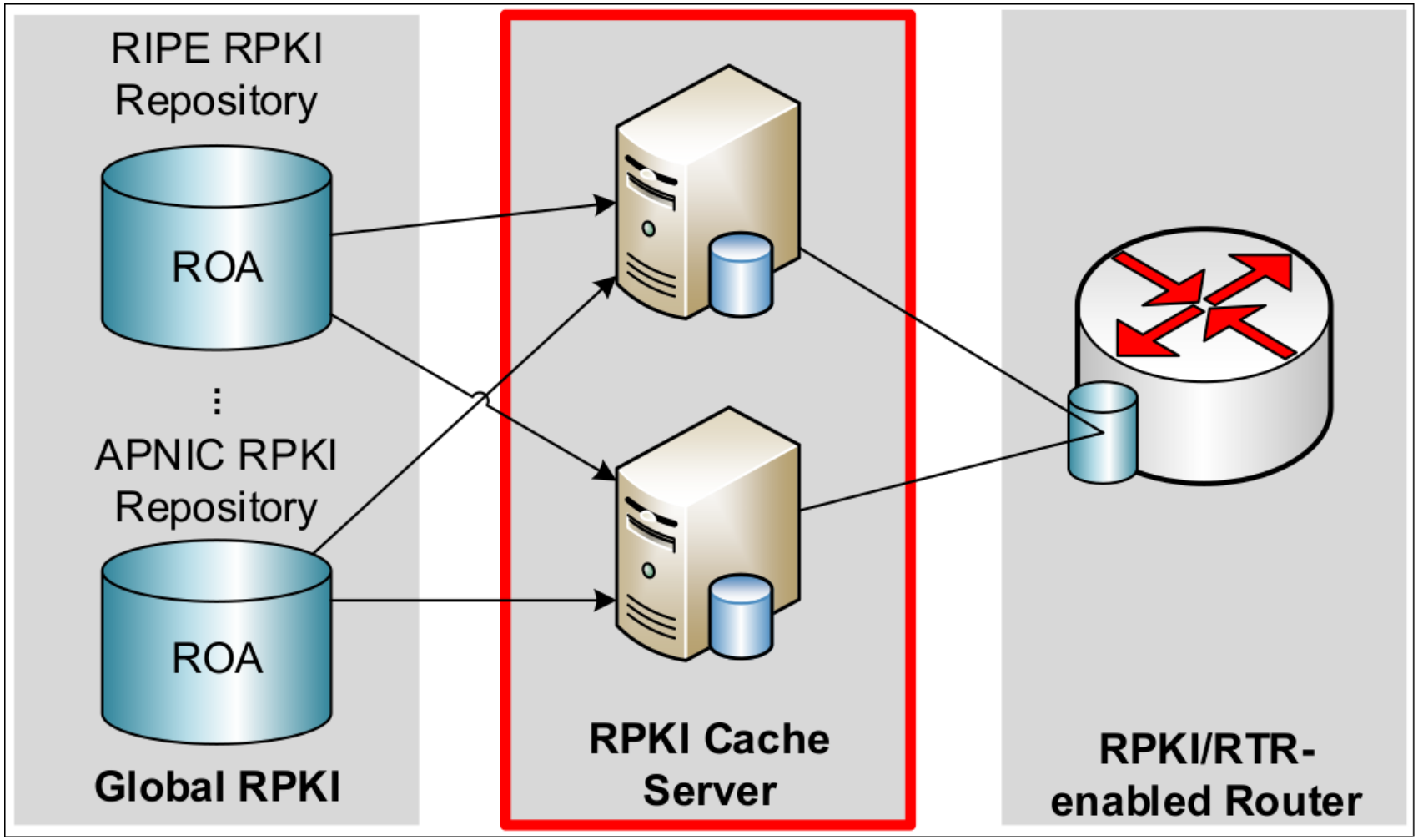
2620:0:2250::/48

75.102.192.0/18

216.220.176.0/20


```
-----BEGIN SIGNATURE-----
CphdY76ofLDDsBzKseuivh9fp8j8f95xZSQrs75MF+GU0nP5OKKtnJ6UvFLZH6L8YEWcxiGGuwTzg
K0Puea+slXnXU+UgalmitqJOHwXbobAm7DCWou2wT2fIWqZHTUpX99/jFlSn34ozp2NFWJCT8ba4W
lNgnIsevnaeoe2KzEUbaawYCOskLU9B7aAPFhBHbuGGhQYpx08n3zLYj1RMIOyOyl8NuSi3cfI0Kb
RZjhtIF3Pe9LebuqrwiBhRaFxzvFLM4g6zDff62/7Hnmt6PFio0Rn1UWPq2plDymT5peluCdDiL3M
/DsGrEgqRfwQKql16HuRKaZVoHa0cNWPdw==
-----END SIGNATURE-----
```

Overview of RPKI validation



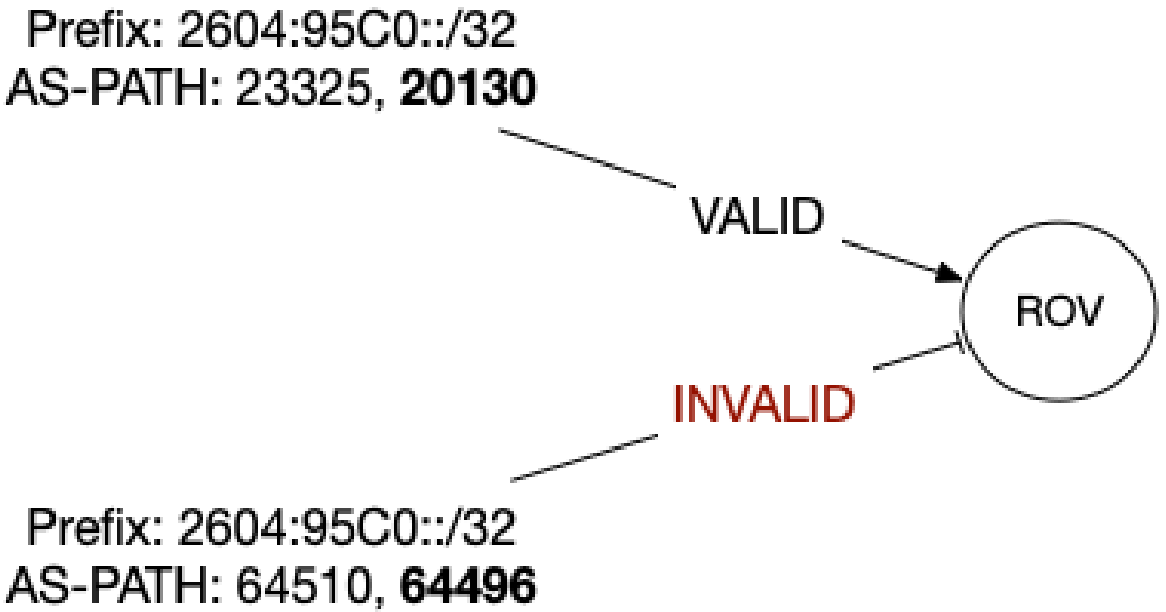
Route Origin Validation (ROV)

ROA Name: DEPAUL AS20130

Origin AS: **20130**

Validity Period: 02-12-2019 to 02-12-2029

Resources: 2604:95C0::/32, ...



RPKI + ROAS → ROV

- RPKI = **repository**
- ROAs = **signed objects**
- ROV = secure routing?

NOTE:

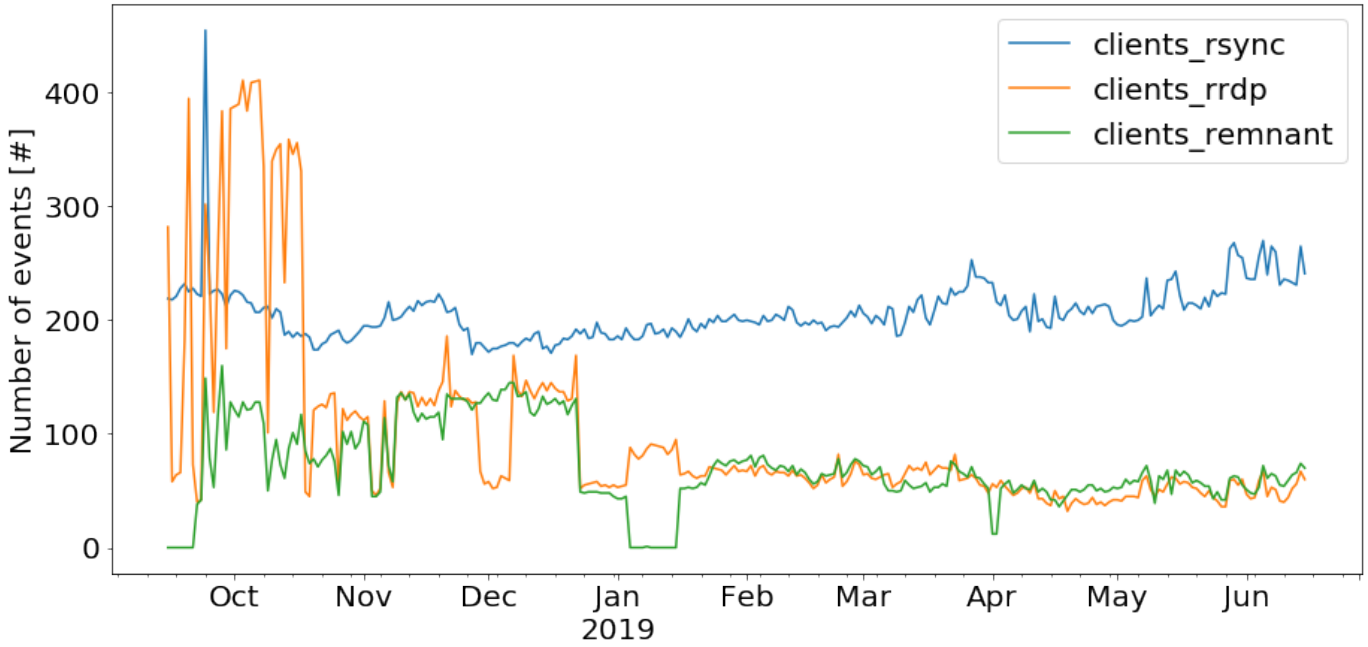
  - ROV only validates “origin” and “prefix”
  - AS-PATHS not protected by ROV
  - ROV is most effective at mitigating accidents

Secure Routing Summary

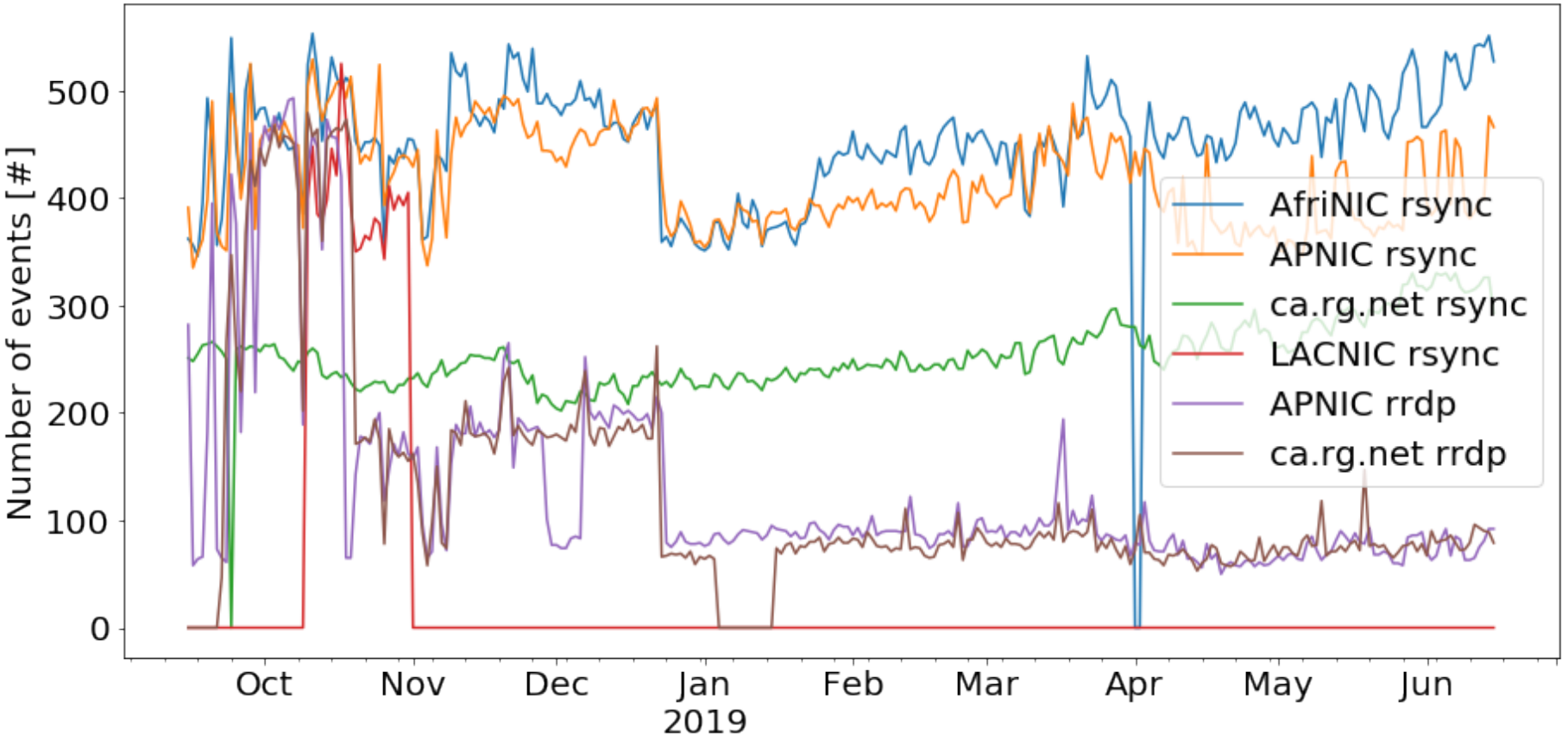
	Utility	Consistency	Ease of Use	Cost
Route Filters	Medium	Low	Medium	Low
Max Limits	Low	Low	High	Low
IRRs	Medium	Low-Medium	Low	Medium
S-BGP / soBGP	High	High	N/A	High
RPKI/ROAs/ROV	**Medium**	**High**	**Medium**	**Medium**

Measurement Design

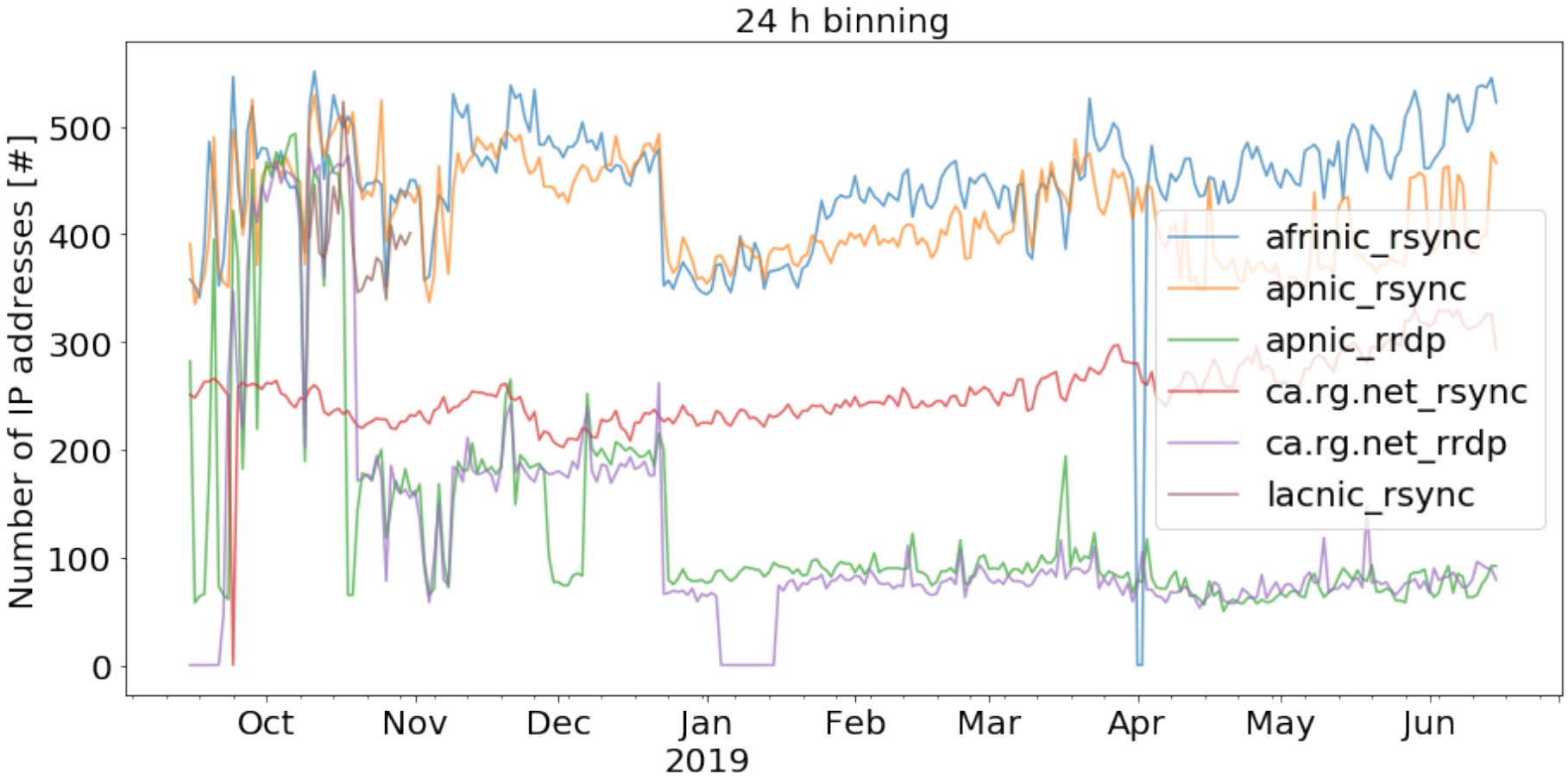
1. Collect trust anchor (repository) access logs
2. Synthesize access method and server identities
3. Analyze (e.g. cache server consistency)



RIR Differences



RPKI Cache Servers



Client Cache and Router Discovery

- Internet Survey
  - rpki-rtr / TCP / 323
  - rpki-rtr TLS / TCP / 324
  - Routinator / TCP / 8282 (documentation example)
  - Junos / TCP / 2222 / “no problem here"
- Passive DNS survey
  - rpki* , [.-]rpki*
- If we could observe rsync traffic to trust anchors
- We see approximately 500 to 1500 client caches

Network RPKI Effects

- A valid ROA is submitted / updated
  - How long before propagation?
  - What are RIR publication frequencies?
  - How consistent are client caches?
- Not all implementations can adequately re-validate
- Caches fetch ROAs at varying intervals
- ROV responsiveness compared to BGP updates

Future Work

- Research project status
  - Data from trust anchors in a database
  - Initial analysis work ongoing
  - Proxy and address aliasing challenges
  - Internet surveys being conducted
  - Beacon versus passive measurement
- Do you find RPKI relevant / useful / interesting?
- What research would be meaningful or useful to you?

Contact Info

- John Kristoff
- Email: jtk@depaul.edu
- WWW: https://aharp.iorc.depaul.edu
- GitHub: https://github.com/jtkristoff/
- Twitter: https://twitter.com/jtkristoff