Routing Security Roadmap

Job Snijders

NTT Communications

job@ntt.net

This presentation contains projections and other forward-looking statements regarding future events or our future routing performance. All statements other than present and historical facts and conditions contained in this release, including any statements regarding our future results of operations and routing positions, business strategy, plans and our objectives for future operations, are forward-looking statements (within the meaning of the Private Securities Litigation Reform Act of 1995, Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended). These statements are only predictions and reflect our current beliefs and expectations with respect to future events and are based on assumptions and subject to risk

Why are we doing any of this?

- Creating filters based on public data, forces malicious actors to leave a trail in IRR, WHOIS or other data sources: **auditability**
- **Bugs happen!** – your router may suddenly ignore parts of your configuration, you'll then rely on your EBGP peer's filters
- **Everyone makes mistakes** – a typo is easily made

Average view on routing security

Perception: it is hopeless, too many holes


TOP 10 VIDEO GAMES FINAL BOSSES
OF ALL TIME

Exhaustive list of issues in the current ecosystem

- IRRdb / database inaccuracy (stale, autopiloted, non-validated)
- IXPs not filtering
- Lack of Path Validation
- Lack of sufficient and good enough software

IRR – what is broken what can be fixed?

- Some IRRdbs do not perform validation
  - Meaning that virtually anyone can create virtually any route/route6 object and sneak those into the prefix-filters

- Eleven relevant IRRs not validating: RIPE, NTTCOM, RADB, ALTDB, ARIN IRR, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE

- Two solutions:
  - Lock the database down (RIPE / RIPE-NONAUTH)
  - Filter on the mirror level

RIPE NWI-5 proposal & implementation

- RIPE NCC's IRR previously allowed anyone to register any non-RIPE-managed space if it had not yet been registered. *DANGER*
- The "RPSL" password & maintainer was used for this

Three steps were taken:

- Cannot register non-RIPE-managed space any more
- All non-RIPE space moved to separate "RIPE-NONAUTH" database
- Route/route6 ASN authorization rules have been improved

More info: https://www.ripe.net/manage-ips-and-asns/db/impact-analysis-for-nwi-5-implementation

OK – so current status

- Ten relevant IRRs not validating: NTTCOM, RADB, ALTDB, ARIN IRR, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE
- Done: ~~RIPE~~

ARIN community also recognized this is an issue

- Consultation at NANOG and through ARIN-Consult mailing list
- https://www.arin.net/vault/resources/routing/2018_roadmap.html
- https://teamarin.net/2018/07/12/the-path-forward/

“Improve, or kill it”

OK – so current status

- Nine relevant IRRs not validating: NTTCOM, RADB, ALTDB, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE
- Done: ~~RIPE, ARIN IRR~~

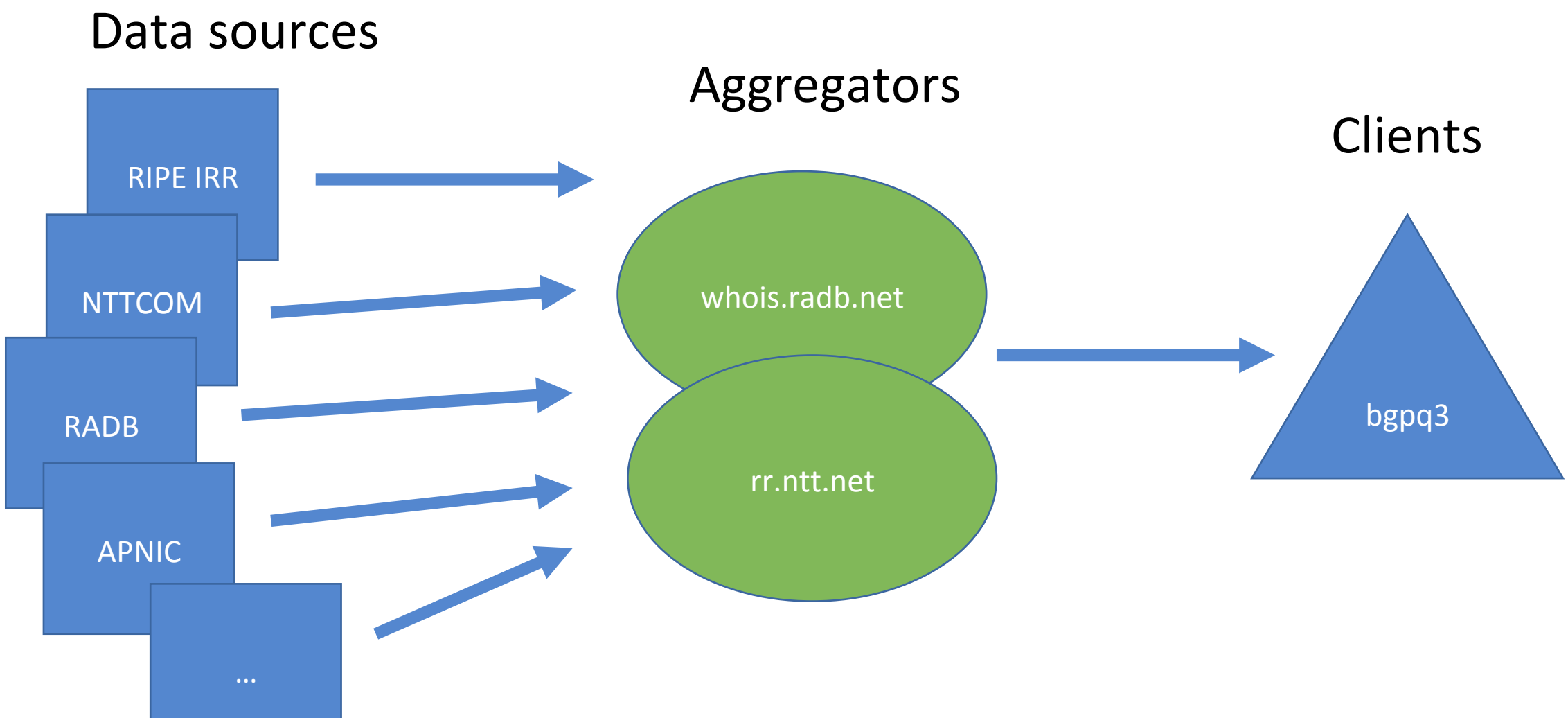
- How to deal with the remaining nine …. ?
- Not all of these are so easily communicated with, not all are really actively managed

The “IRR” system access

- The IRR is access through predominantly two “gateways”
  - **`whois.radb.net`** (the bgpq3 and peval default)
  - **`rr.ntt.net`**
- All mirroring is essentially done with one software: IRRd

Solution: Let’s use the hegemonic duopoly for good!

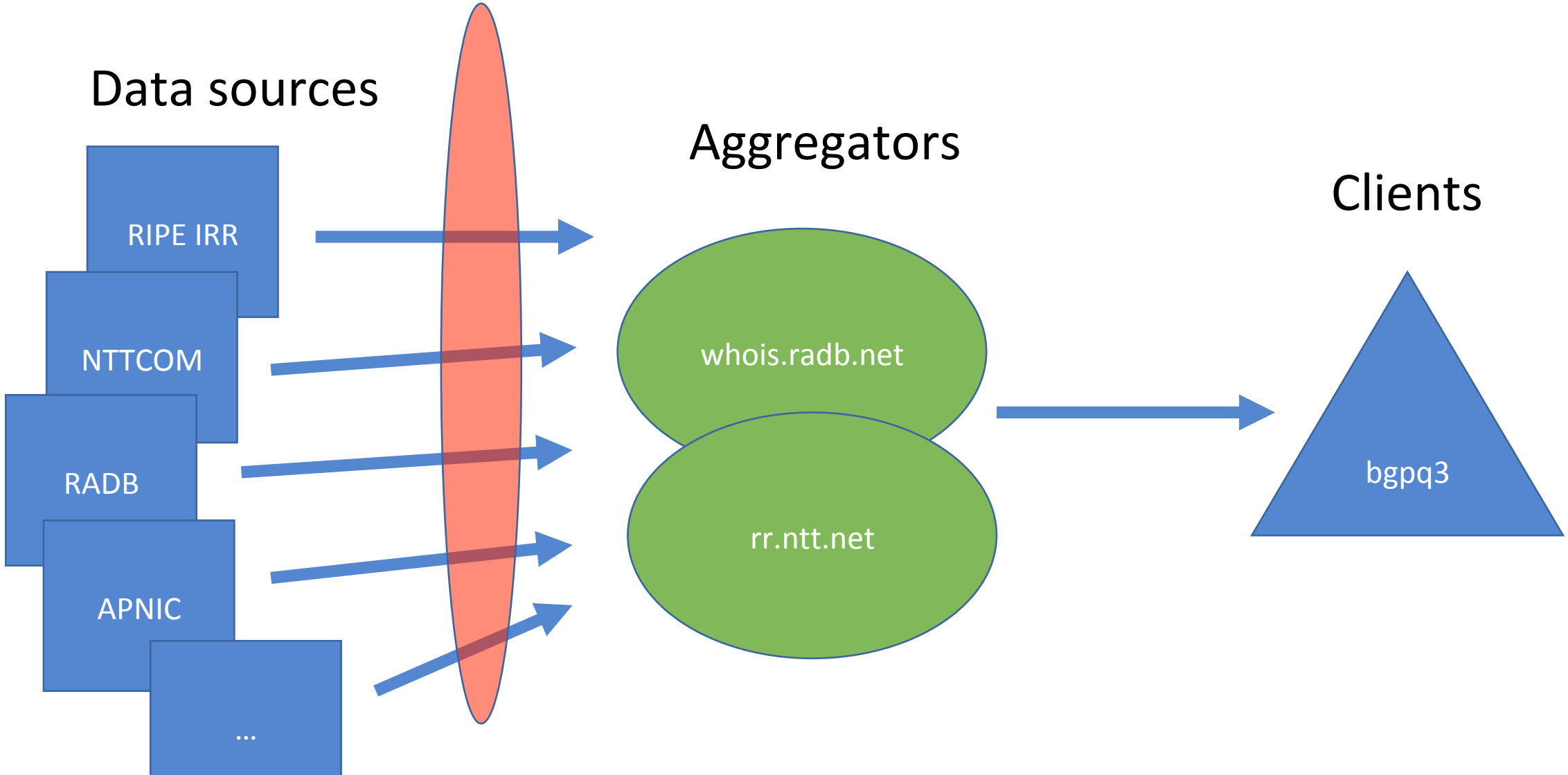
Improving security at the ”aggregator”?



Proposal: Let RPKI “drown out” conflicting IRR

- RPKI can be used for *BGP Origin Validation* – but also for other things!
- A RPKI ROA is sort of a route-object
  - It has a “prefix”, “origin” and “source” (the root)
  - We can use RPKI ROAs for provisioning BGP prefix-filters
- Extend IRRd so that when IRR information is in direct conflict with a RPKI ROA – the conflicting information is suppressed (Github)

RPKI filter at the aggregators



RPKI suppressing conflicting IRR advantages

- Industry-wide common method to get rid of stale proxy route objects – by creating a ROA you hide old garbage in IRRs
- By creating a ROA – you will significantly decrease the chances of people being able to use IRR to hijack your resource

OK – so current status

- IRRs not validating: no longer relevant

- Done: ~~RIPE, ARIN IRR, NTTCOM, RADB, ALTDB, BBOI, BELL, LEVEL3, RGNET, TC, CANARIE~~

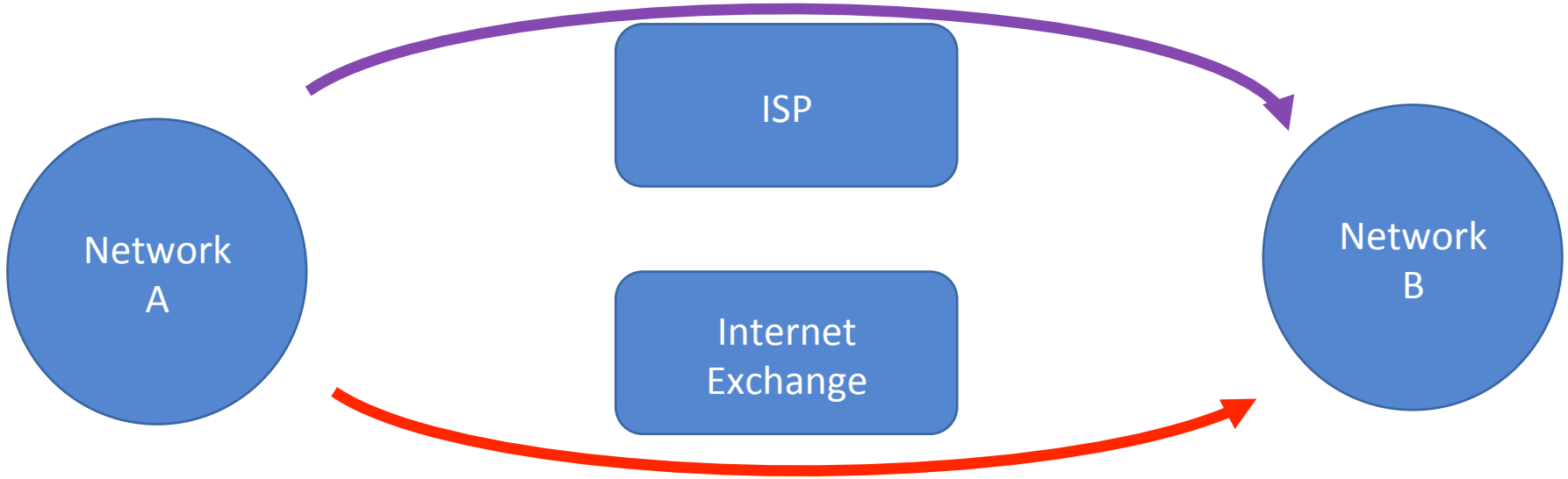
NTT & Dashcare have started a full rewrite of IRRd to make this possible: https://github.com/irrdnet/irrd4

”Filtering at IXPs is hard”

- Many IXPs have come to realize their responsibilities to the Internet ecosystem and the commercial benefits of a more secure product.
- http://peering.exposed/
  - 9 out of top 10 IXPs are filtering, tenth will later this year. **IX.br** making good progtress
- IXP filtering has become much easier, there are multiple fully featured configuration generators:
  - https://www.ixpmanager.org/
  - http://arouteserver.readthedocs.io/
- BIRD’s hegemony in the route server software is being challenged: OpenBGPD is funded to be able to compete

Route servers must begin dropping RPKI Invalids

- Route servers *by definition* provide partial Internet tables
- No guarantees whatsoever that a given route will be available via RS
- When a route server drops a prefix, **worst case scenario is rerouting** – not an outage.



Not everyone needs to do RPKI

- Because of the centralization of the web, if a select few companies deploy RPKI Origin Validation – millions of people benefit
- (google, cloudflare, amazon, pch/quad9, facebook, akamai, fastly, liberty global, comcast, etc…)
- I think only 20 companies or so need to do Origin Validation for there to be big benefits…
- https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/

“RPKI Origin Validation is useless without Path Validation aka BGPSEC”

- The lack of path validation can be resolved through two methods:
  - Densely peer with each other (Example: Google & Akamai have 126+ facilities in common with each other)
  - An AS_PATH blocking mechanisms like “peerlock”
- Both effectively are “path validation for 1 hop”
- Perhaps “1 hop” already is good enough ☺

“There is no healthy software ecosystem”

- RIPE NCC Validator v3 is works and actively maintained
- NLNetlabs is writing a RPKI Cache Validator (Routinator 3000)
- A company I can’t name is secretly writing one too

- Almost all serious routing vendors have RPKI support (Cisco, Juniper, BIRD, Nokia, FRR – and more are on the way)

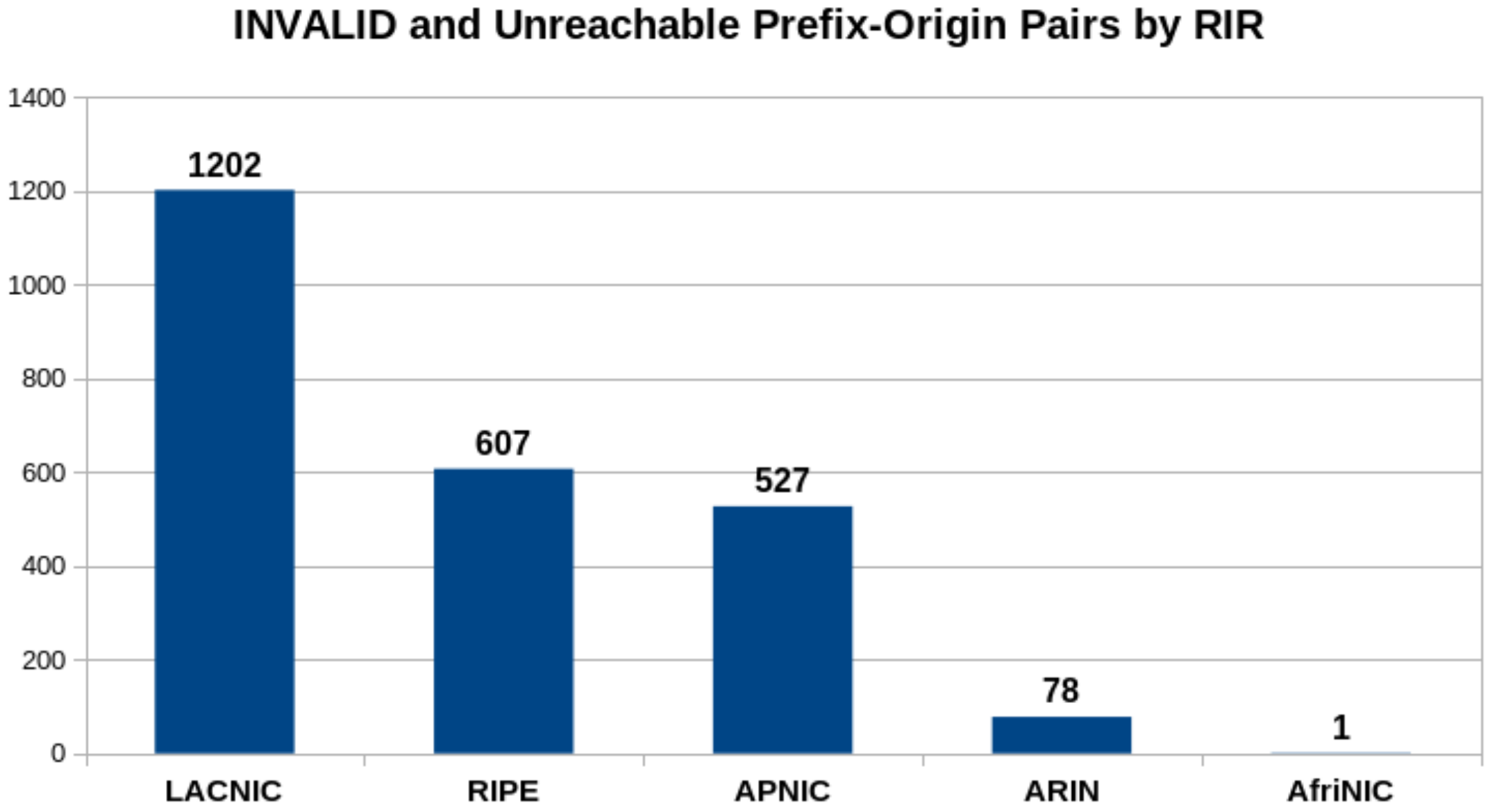
- Solution: more users results in better software, start using!

Timeline

- IXPs – start doing RPKI Origin Validation on your route servers **now**
- ISPs / CDNs
  - if you are pointing default somewhere, do it **now**
  - If you are transit-free, wait a bit

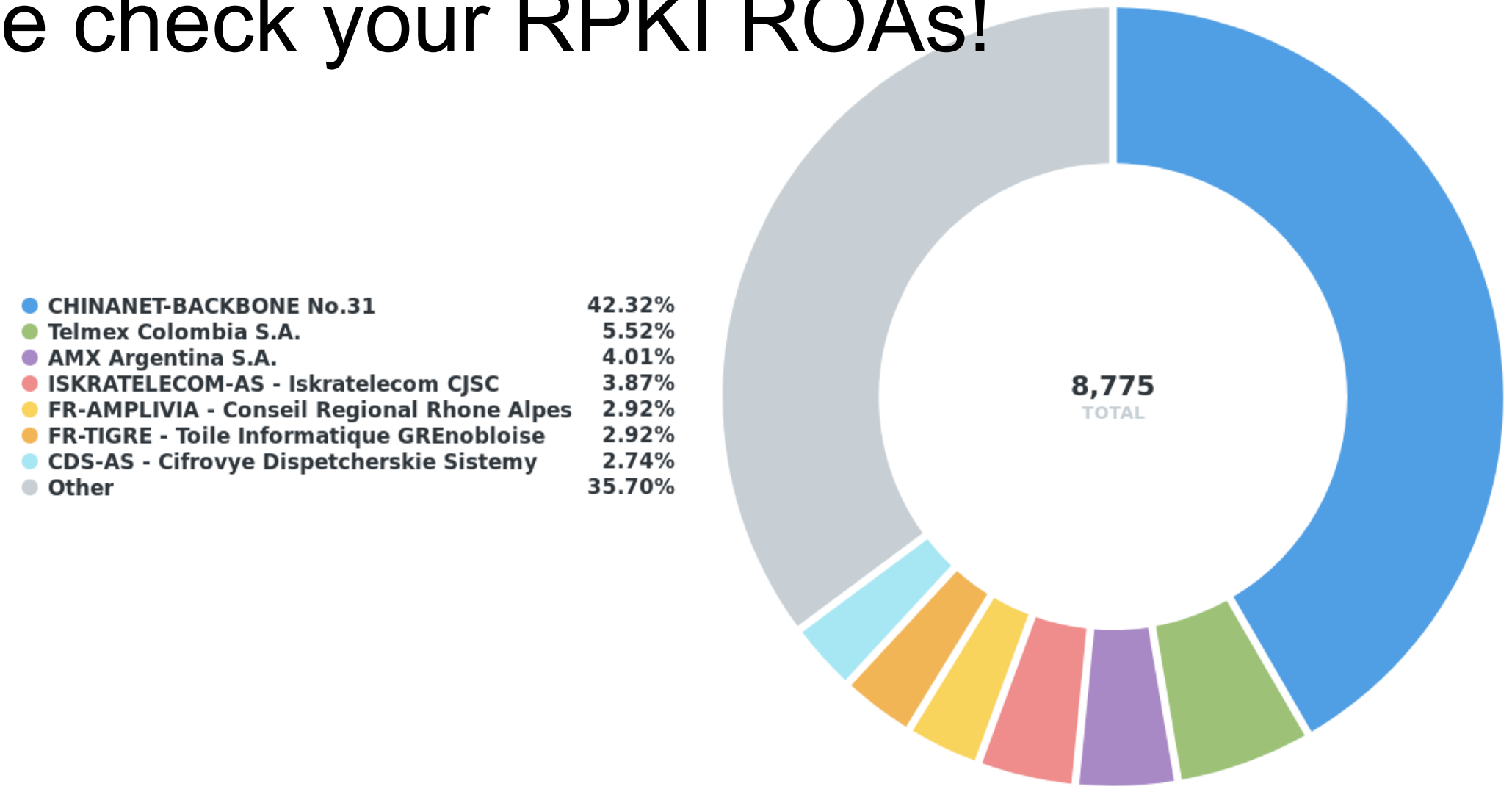
We aren’t done yet - Future work

- Use the RPKI to publish “peerlock” rules about who are authorized upstreams and who aren’t
  - https://tools.ietf.org/html/draft-azimov-sidrops-aspa-verification
  - https://tools.ietf.org/html/draft-azimov-sidrops-aspa-profile
- Extend the RPKI to replace IRR AS-SETs (IRR / RPKI feature parity)
  - https://tools.ietf.org/html/draft-ss-grow-rpki-as-cones
- ARIN TAL issue needs addressing



Source: https://medium.com/@nusenu/towards-cleaning-up-rpki-invalids-d69b03ab8a8c

Double check your RPKI ROAs!



Source: https://medium.com/@nusenu/where-are-rpki-unreachable-networks-located-65c7a0bae0f8

Conclusion


QUESTION
THE
ANSWERS