Measuring RPKI ROV deployment and edge cases

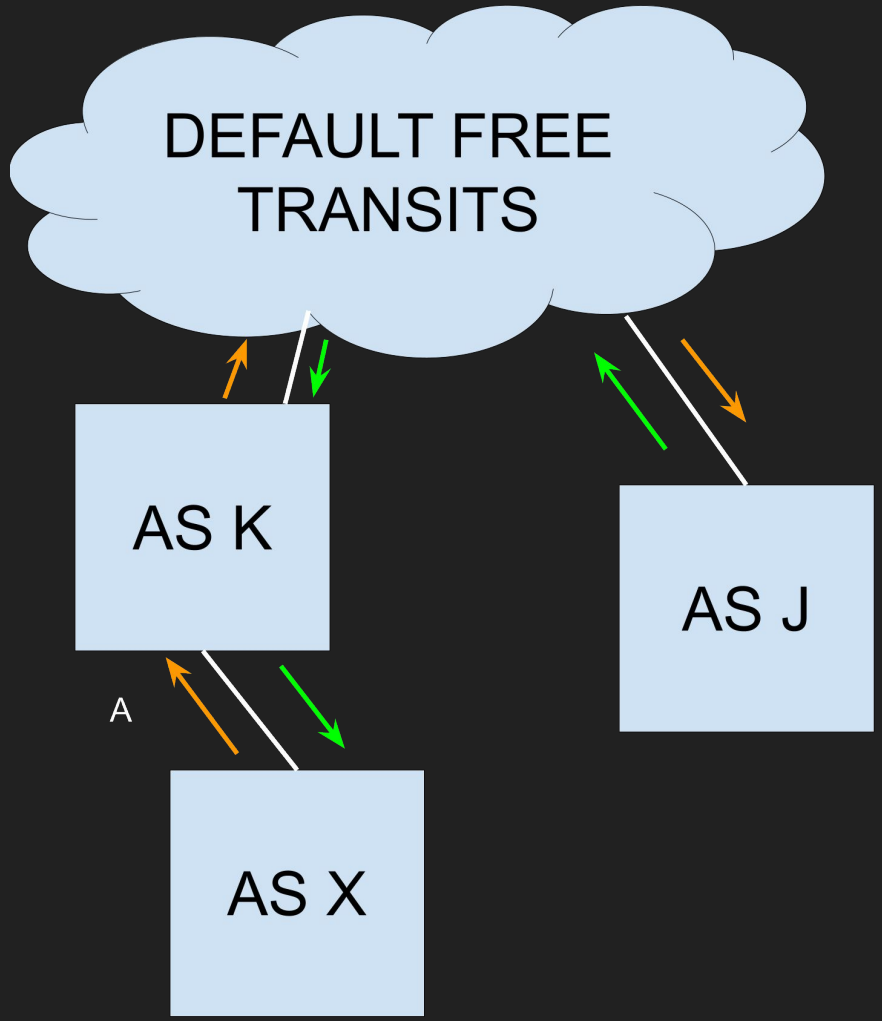
June Slater

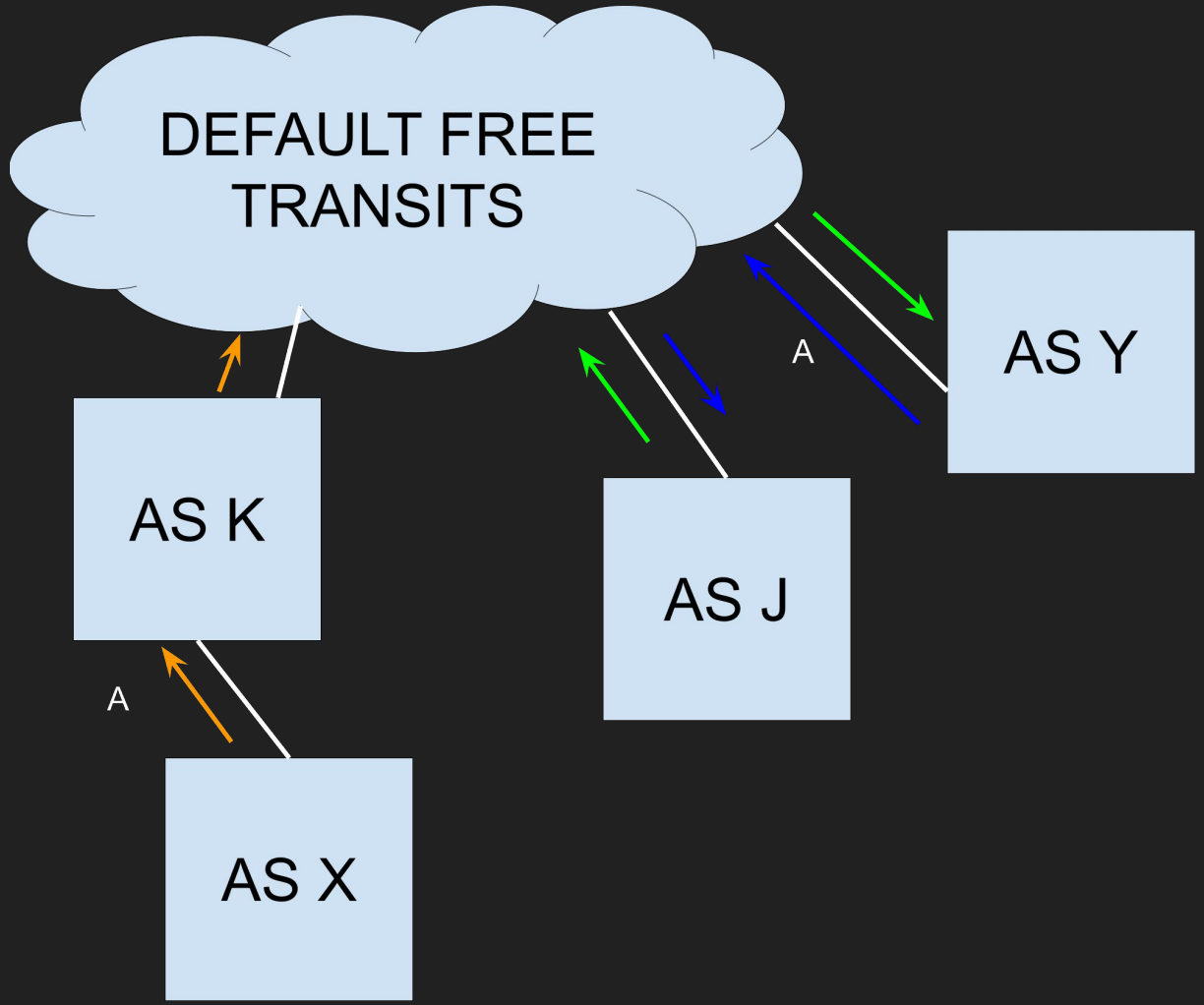
Disclaimer

All opinions expressed in this presentation represent my own views and do not necessarily reflect the views of my employer.

A discussion of trends

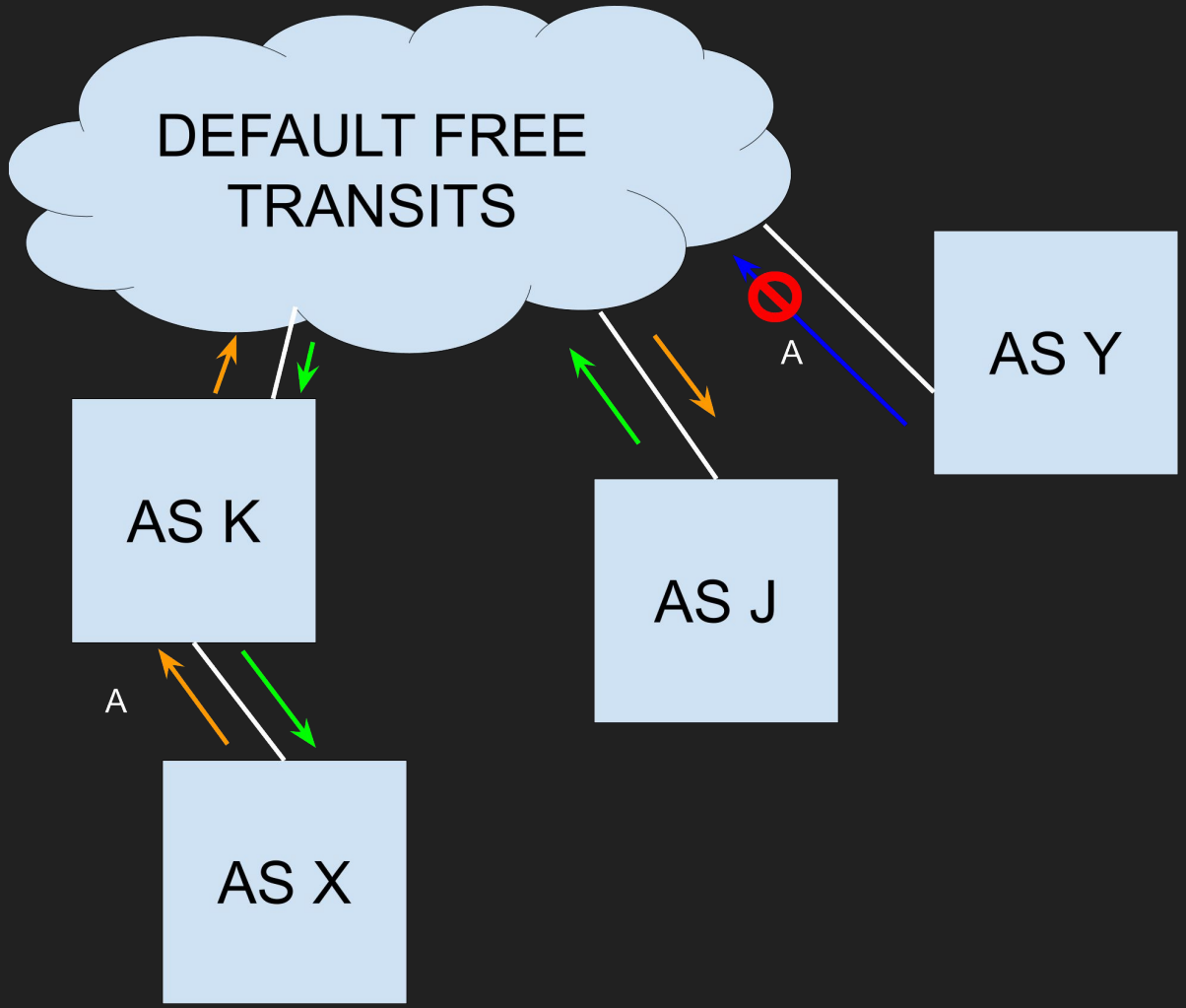
- All methods that are discussed have implicit (and in some cases quite significant) data biases
- This is not an academic study, but rather intended to highlight trends, patterns, and other relevant happenings


DEFAULT FREE
TRANSITS
AS K
AS J
A
AS X


DEFAULT FREE
TRANSITS
AS K
AS J
AS Y
AS X
A
A

ASN X
MAY ANNOUNCE
PREFIX A
OF SIZE /24

- YOUR RIR


DEFAULT FREE
TRANSITS
AS K
AS J
AS Y
AS X
A
A

What RPKI ROV prevents

- Fat-finger announcements
- De-aggregated announcements using a modified source ASN
  - AS7007 incident
  - Some BGP optimizers
- Direct hijacks not involving origin AS spoofing
  - September 2020 politically-sensitive re-route incident
  - April 2018 DNS re-route incident

What RPKI ROV does not prevent

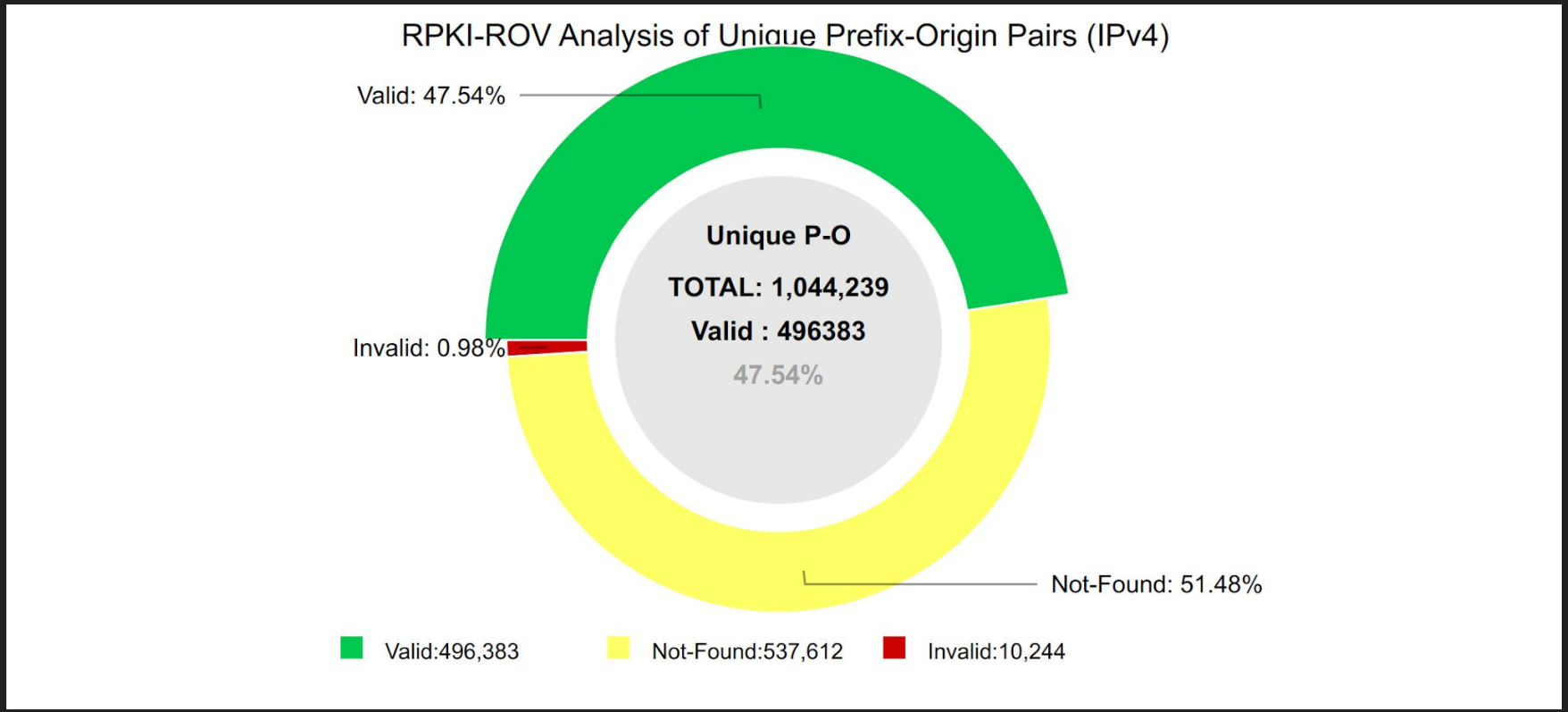
- Some de-aggregated announcements with source ASN manipulation
  - July 2019 BGP optimizer incident
  - Can be prevented using ROV based on RPKI max length
- Direct hijacks involving path manipulation
  - November 2018 regional cloud provider incident
  - October 2017 DPRK Incident

What it prevents is still valuable

Quickly checking the Wikipedia list of known incidents:

- ~85% (18/21) would be prevented by RPKI ROV
- Most that succeeded would have been much less consequential with RPKI ROV
  - Adding more ASes to the path will decrease the chance that a prefix hijack wins the traffic
- Attribution (i.e. “was this intentional”) becomes clearer

It’s (kind of) being signed!



Methodology - looking via the dataplane

- Take an ARIN and RIPE-allocated /24
- Announce it via your friendly local ISP
- Ping sweep the internet from the prefixes, see what comes back
- Invalidate the existing RPKI signatures
- Wait for 24 hours
- Re-run the baseline test

and it (naively) looks like it’s being validated!

Methodology - looking via the dataplane, try 2

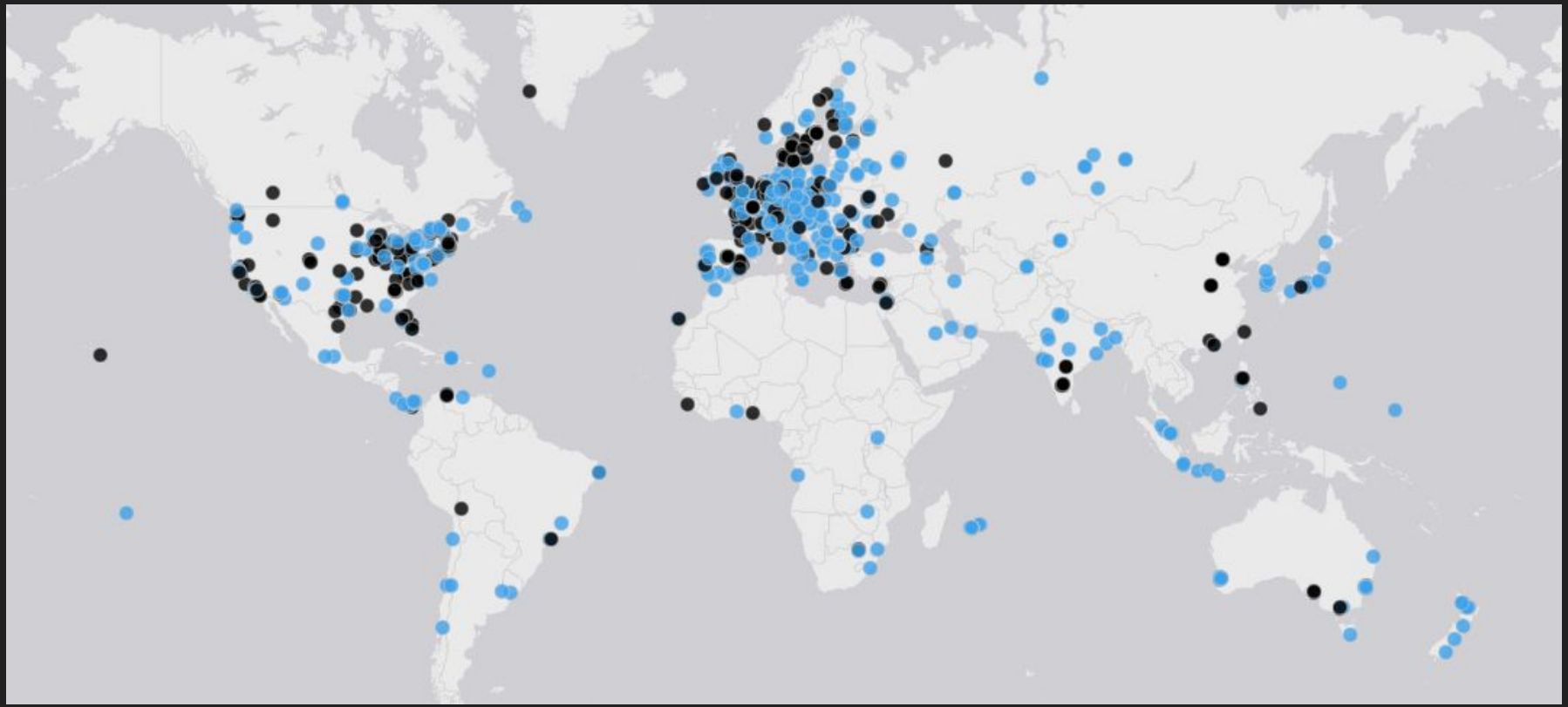
Perform the same test, except:

- Announce it via a large, well-peered network
- Perform a baseline:
  - Attempt to reach the IPs using RIPE Atlas probes
  - Attempt TLS issuance, test DNS resolution, etc…

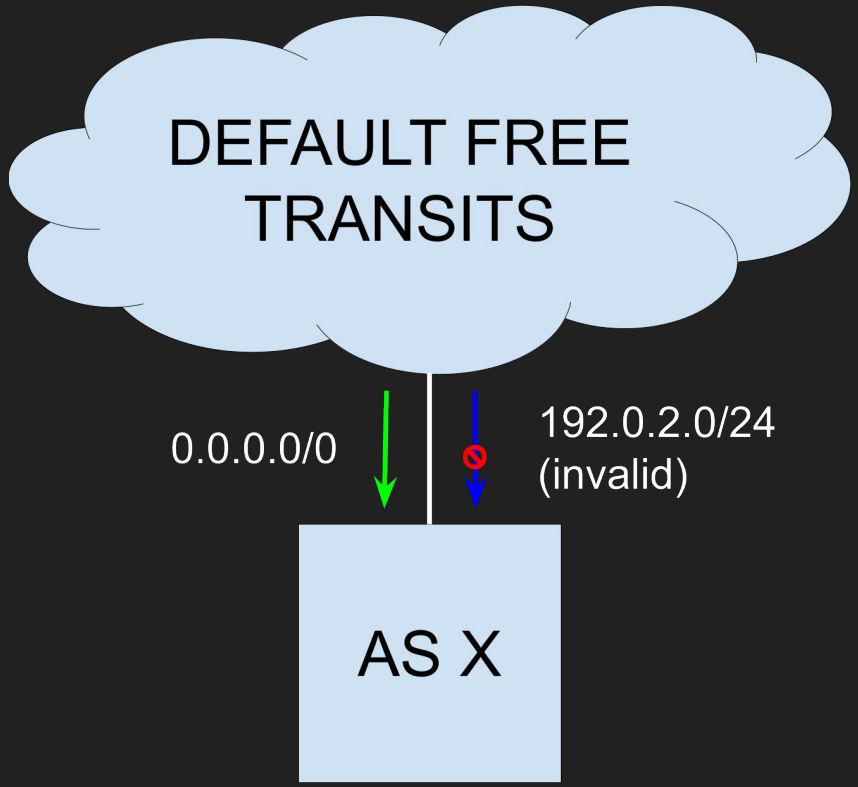
RPKI ROV’s Pareto point

- “Not everyone needs to do RPKI” - if the critical 20% actually sign and validate using ROV, we will see the majority of the benefit.
- Previously hypothesized: cloud hyperscalers, public DNS services, CDNs, and large scale consumer networks

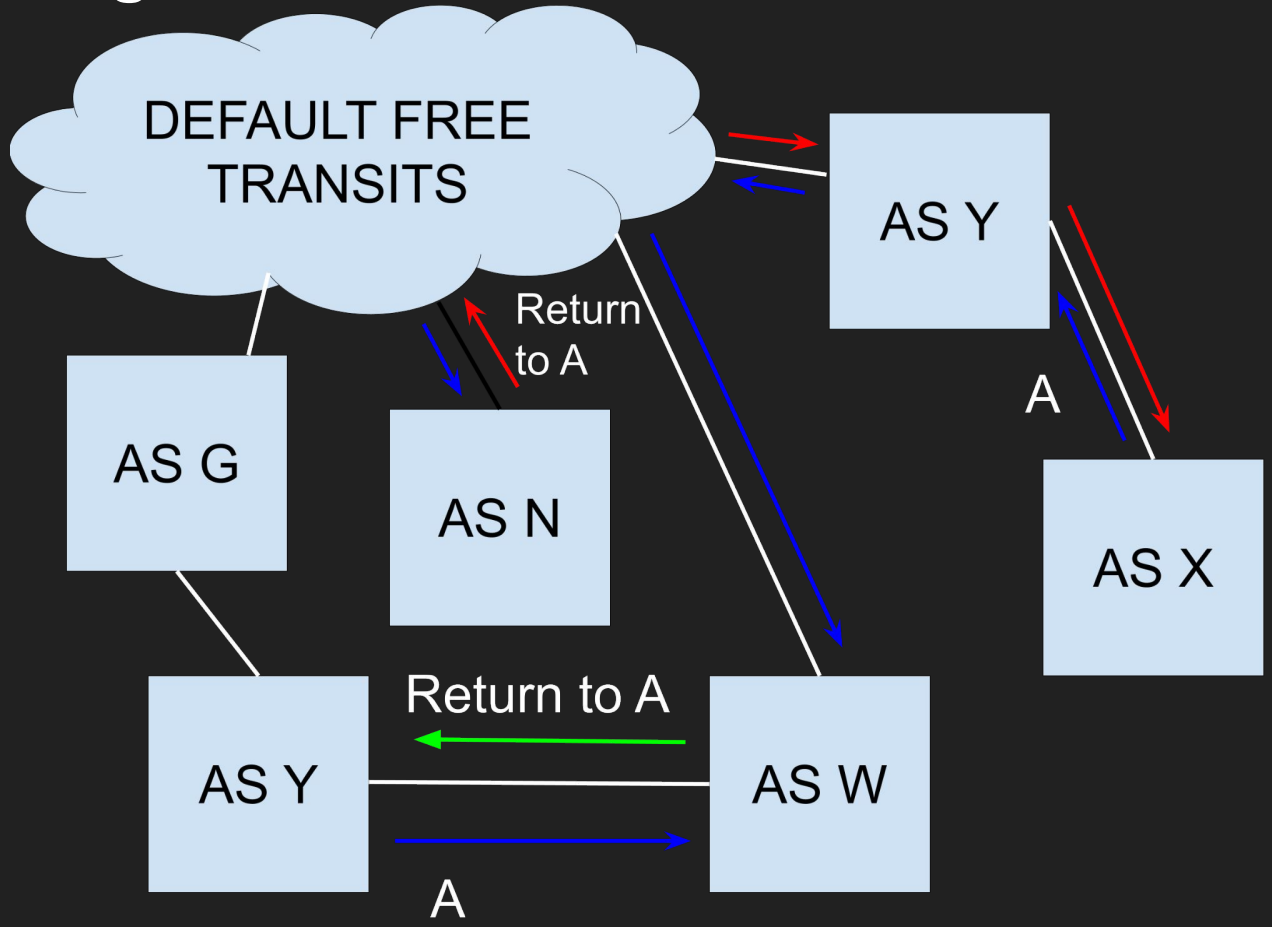
The “protection” of your upstreams



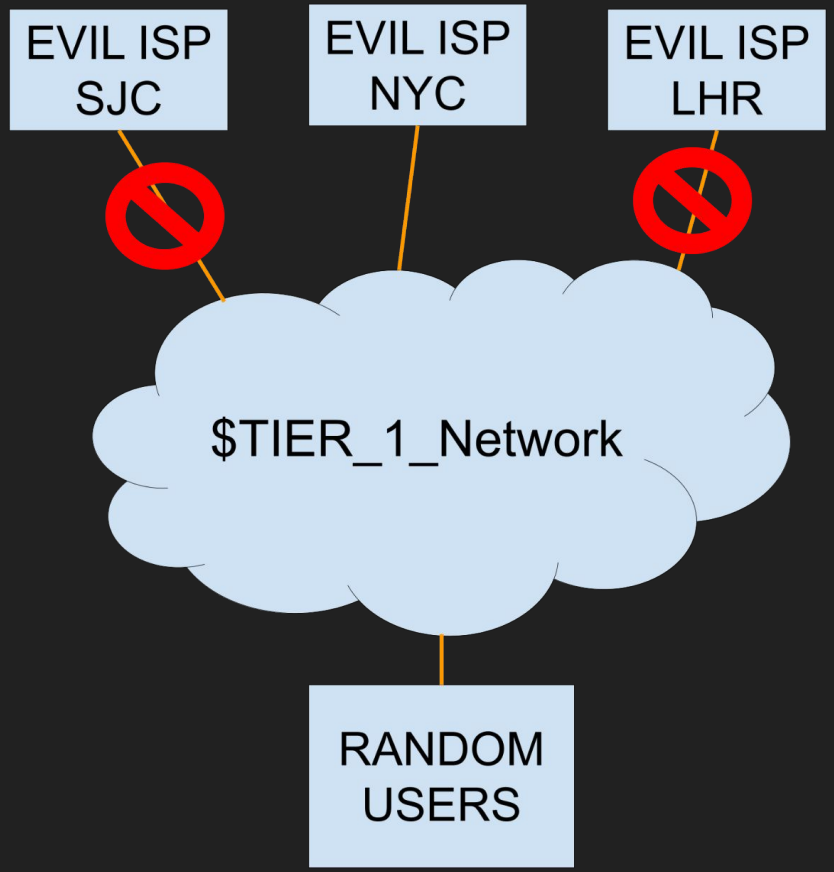
Is it a default route?



Is it peering?



Is it a single router that isn't enforcing ROV?



General observations

Looking at 100 random probes from each latency delta quartile:

- Very few probes (6 observed) had potential default routes.
  - Non-IX, ISP/carrier ASN as the next hop

cont…

General observations (cont.)

- Probes with a higher latency delta tended to go via transit to a single unfiltered port (on a provider that claims to filter everywhere) - *~36% of the probes*
- Probes with a similar latency delta tended to stay on an identical (or similar) peering path.

The ARIN TAL

- The distribution of the ARIN TAL was restricted until September 2022.
- After September 2022, it was generally available to be included by default.
- How have things changed?

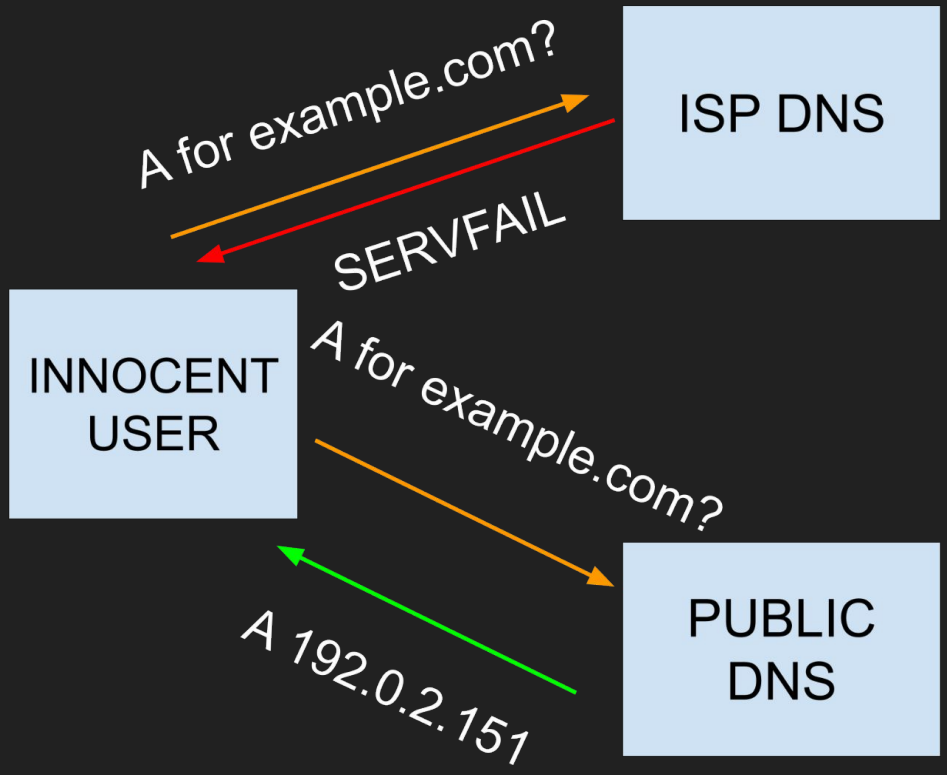
The ARIN TAL

- 2018, Ben Cox: difference is ~ 100,000 IPs, or 0.038% of the total sample
- 2023: total difference is ~ 120 probes, or 1.8% of the total sample
- If cloud providers are removed from just the Americas portion of the sample, difference is ~ 0.051% of the total sample.
- Not a significant change from the 2018 data
- Overall connection rate for RPKI invalids of ~64-66%

DNS Providers

- Public DNS providers - with one exemption - generally failed to validate.
- When a home or business ISP validated, their DNS providers generally validated and did not respond to invalid requests.
- 78.63% of probes received a DNS response from a DNS server that resided inside of a RPKI-invalid route

DNS Providers



TLS authorities

- Implicitly reliant on routing security for domain validation
- Several different ways to validate
  - Each mode has several failure positions (does it fail to resolve due to the nameserver being RPKI invalid? Does it fail to reach a RPKI-invalid mail server? etc…)
- Two certificate authorities issued certificates:
  - One issued a certificate based on RPKI-invalid DNS
  - One issued certificates to both DNS (dns-01) and HTTP (http-01)

TLS authorities - observations

- One large authority was “saved” by their reliance on a cloud provider that filters
- The authority that issued on the basis of DNS queried from an atypical host in Asia (several minutes slower than it normally would have been).

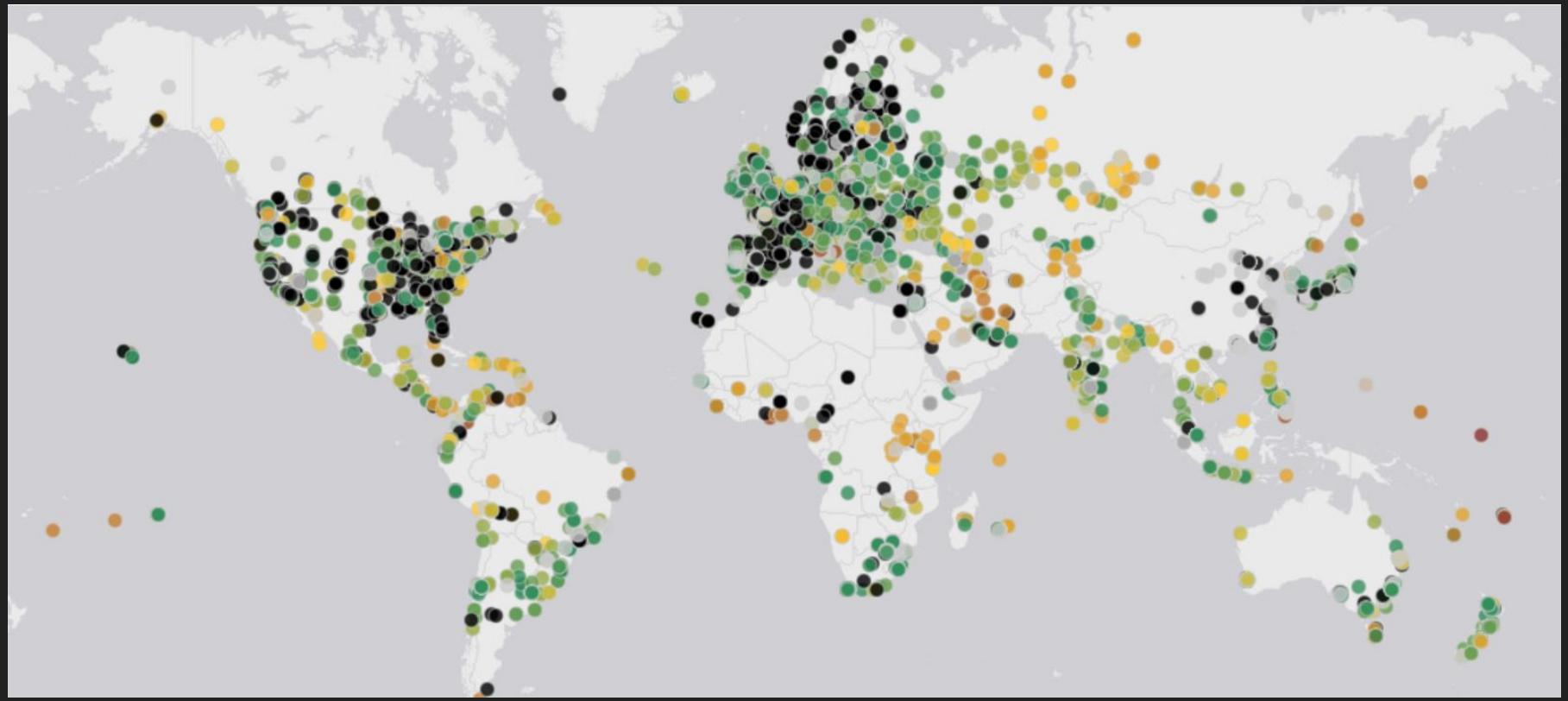
Long-term data collection - Cloudflare's test prefix

- April 2020: Cloudflare launches isbgpsafeyet.com to test validation
- Uses 103.21.244.0/24 to test connectivity in the user's browser
- Tool encourages users to Tweet at their ISP about the issue

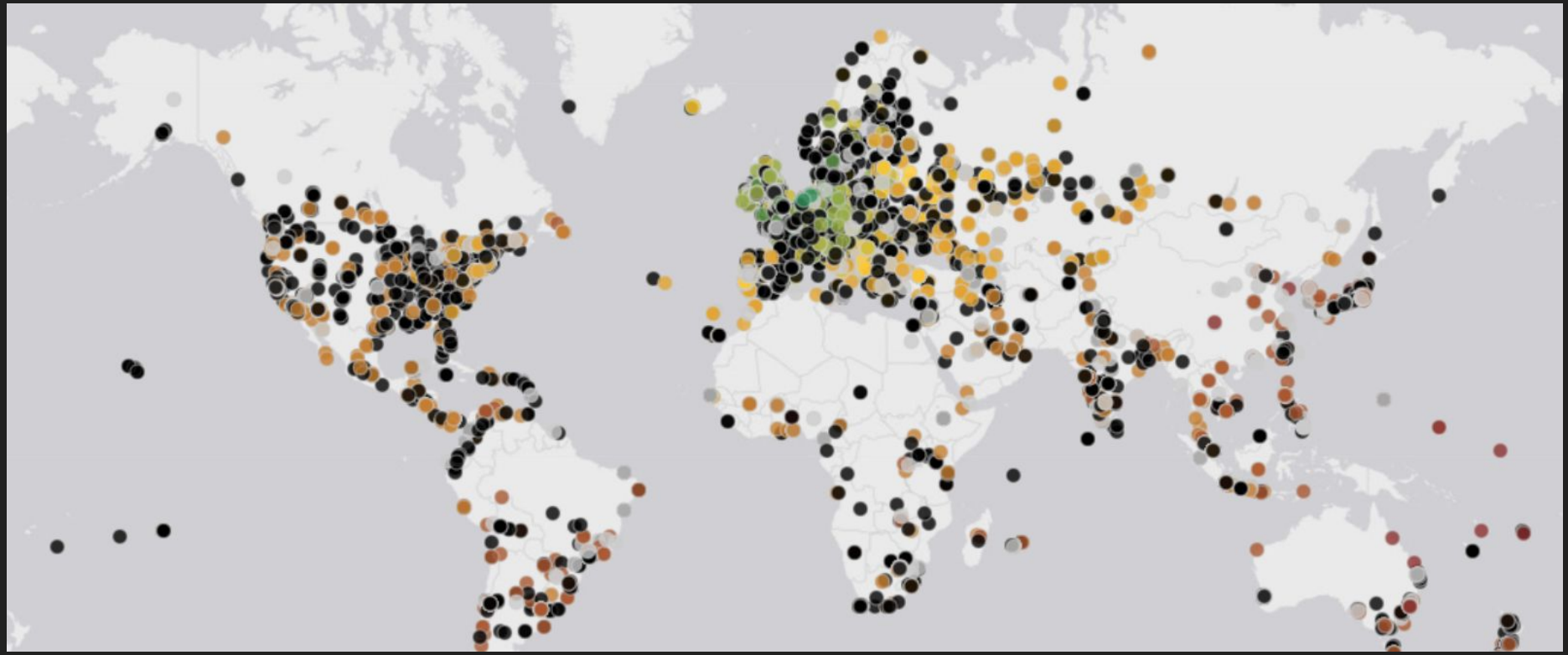
Long-term data collection - Cloudflare’s test prefix

- ARIN test prefix: overall connection rate (post-de-noise): 66.16%
- RIPE test prefix: overall connection rate (post-de-noise): 64.36%
- Cloudflare’s RPKI invalid test prefix: 65.41%
- Likely not manually blocked, at least not at scale.

Long-term data collection



Long-term data collection



Takeaways

- Deployment is happening, and it’s got impact
- Filtering peers is now arguably more important than filtering upstreams

…though upstreams need to be thorough!

Takeaways

- Think about routing security (and the tools that can help ensure it) in your threat model
- Ongoing measurement can safely use public RPKI testing prefixes.
- Legal changes to the ARIN TAL simplify deployment, though they didn’t have a visible impact on validation.

Questions?

E-mail @ june at rezero.org

Thank you to the RIPE Atlas team for the use of the Atlas network!