Infrastructure Geolocation & Openness vs. Security
Part I
RIPE IPmap
RIPE IPmap

- We now have a first production version of our infrastructure geolocation service
  - https://ipmap.ripe.net/
  - It’s in a very early stage, needs more work to really make it useful
  - Focus was on getting API basics done
  - Comes with a UI (separate and included in RIPE Atlas)
RIPE IPmap

Geolocating Internet Infrastructure

212.147.63.218

146.66.232.10  Jönköping, SE-08 Sweden
2a01:488:bb::163  Frankfurt am Main, DE-05 Germany
212.147.63.218  Zürich, CH-ZH Switzerland
RIPE IPmap

- It can combine multiple inputs to calculate geolocation probabilities
- It can provide the “single best answer” and all alternatives as well
- Current engines include:
  - “single radius”: “triangulation” with RIPE Atlas probes
  - “simple anycast”: anycast detection from anchors
  - “crowdsourced”: user supplied input
RIPE IPmap

• Plans for future engines include:
  • Reverse DNS
  • Alias resolution?
  • Proximity?
  • maybe more
• Also, support for “more specific” queries
• Perhaps a “visualise this trace” feature
Part II
Openness vs. Security
Inspiration

From “topics of interest”:

- Future measurement infrastructure architectures
  - resolving tensions between openness and security of measurement platforms
RIPE Atlas Software Probes

- There’s demand to support this
- It allows growth in networks that are otherwise unreachable by physical probe installation
- But it has challenges too
  - Clients are unverifiable, increased risk of malicious probe — needs more attention to detect bad behaviour
  - What’s the value of having more probes in already saturated networks?
RIPE Atlas Software Probes

- How to steer deployment of new probes into desired networks?
- Should there be a vetting procedure for new hosts?
- Need to void “fast flux probes”
- Do we need to deal with client platform differences?
Fair Share

- RIPE Atlas is a multi-user network, we need to enforce reasonable use
- Probes can deal with thousands of measurements running, but the hosts’ networks may be affected
- Each measurement has a cost on the infrastructure too
- Therefore there are quotas defined on number of measurements and involved probes, per user
- Ultimately we want to use a metric based on “total strain” on the network
Ethical Considerations

- One also needs to protect the hosts from misuse
  - See enforcing quotas before
  - Also, what kind of measurements are available from the probes is limited
    - E.g. HTTP is available but only towards anchors
    - There is probably more risk higher up in the network stack - but it’s getting fuzzier by the day (DoT, DoH, QUIC, …)
  - We published guidelines for ethical considerations
Questions