University of Glasgow

Internet Protocols Laboratory

AS112 Deployment Characteristics and Security

Elizabeth Boswell, Xinyan Xian, Mingshu Wang, Stephen McQuistin, Colin Perkins

University of Glasgow

What are junk queries?

- Not all DNS queries have a meaningful response
  - “What domain name resolves to 192.168.0.1?” → private address, so no meaningful answer
  - Sent by misconfigured software
- **Where do those junk queries go?**
  - Are answered by **AS112**

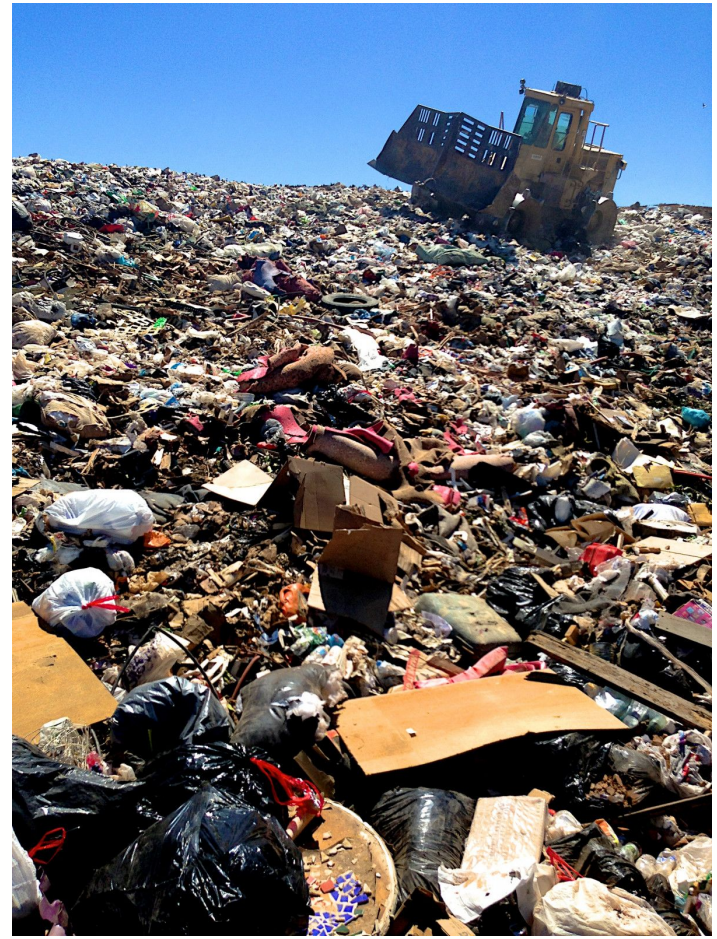
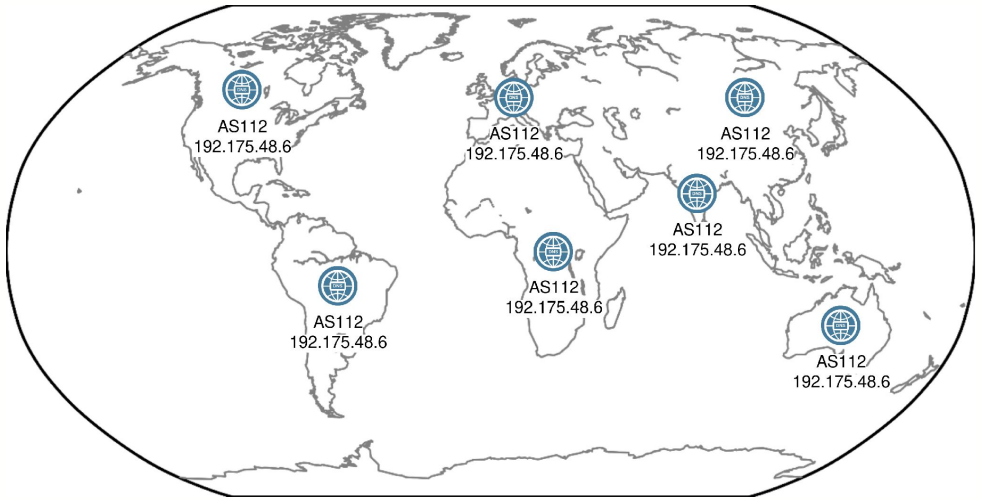


Image by Alan Levine, https://pxhere.com/en/photo/213020

What is AS112? (1)

- **AS112:** anycast DNS deployment that captures junk queries
  - Diverts them from .arpa/in-addr.arpa nameservers
  - Nameserver for reverse mappings of RFC1918 private addresses and link-local IPv4 addresses, home.arpa and service.arpa
    - Reverse mapping: 203.0.113.23 → 23.113.0.203.in-addr.arpa
    - Reverse DNS (rDNS) query: PTR query for the reverse mapping



What is AS112? (2)

- AS112 is a volunteer-run network
  - **Anyone** can add a site without prior coordination or permission
  - “Loosely coordinated” by DNS-OARC, maintains self-reported list of operators (as112.net)

University of Glasgow

What we don’t know...

- We don’t know:
  - **Who** runs AS112 sites?
  - **Where** are these sites located, and how does AS112 perform?
  - **What** traffic does AS112 receive? Are there any security risks?
- Why study AS112?
  - Queries sent to AS112 can contain **sensitive information**, e.g. hostnames or service queries, which could be **received by anyone**
  - **Protects** important parts of the DNS, needs to be resilient
  - Uniquely uncoordinated DNS deployment

University of Glasgow

This talk

- Will present results from **two research studies**
- First: study of AS112 deployment characteristics
  - Black Holes and Prisoners: Understanding AS112 Deployment Characteristics (https://doi.org/10.1007/978-3-032-18268-5_9)
- Second: study of the privacy and security risks of AS112 traffic (work in progress)

University of Glasgow

- **Part 1: AS112 Deployment Characteristics**
  - Our Methodology
  - Who runs AS112?
  - Where is AS112?
  - Comparison with DNS root

University of Glasgow

Research Questions

- We want to know:
  - **How many** AS112 sites are there? **Who** runs them?
  - **Where** are they **located**? From where are they **accessed**?
  - How does it **compare** to other anycast networks?

University of Glasgow

Our measurements

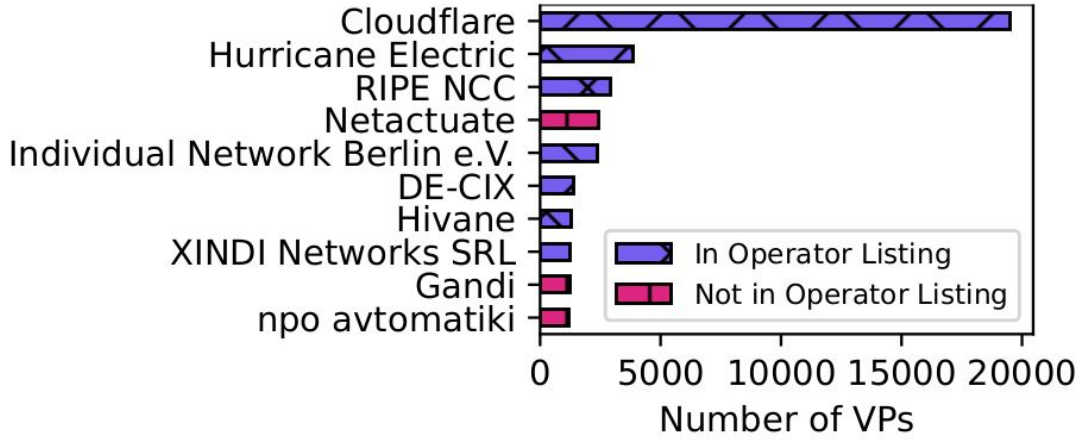
- AS112 sites respond to TXT queries for **`hostname.as112.arpa`** or **`hostname.as112.net`** with information about their **location and operator**

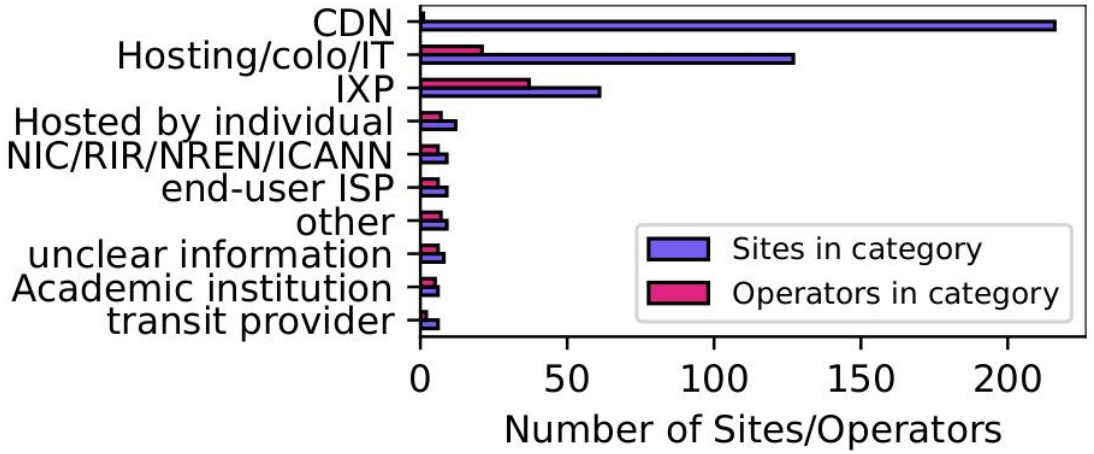
```
el@camorta:~$ dig +short TXT hostname.as112.arpa
"RIPE NCC, Amsterdam, The Netherlands"
"See http://www.as112.net/ for more information."
```

- By sending such queries from a large number of vantage points, we can find a large number of sites
  - Sent **hostname** queries from 11,973 **RIPE Atlas probes** and 33,646 **open recursive resolvers**

Who runs AS112?

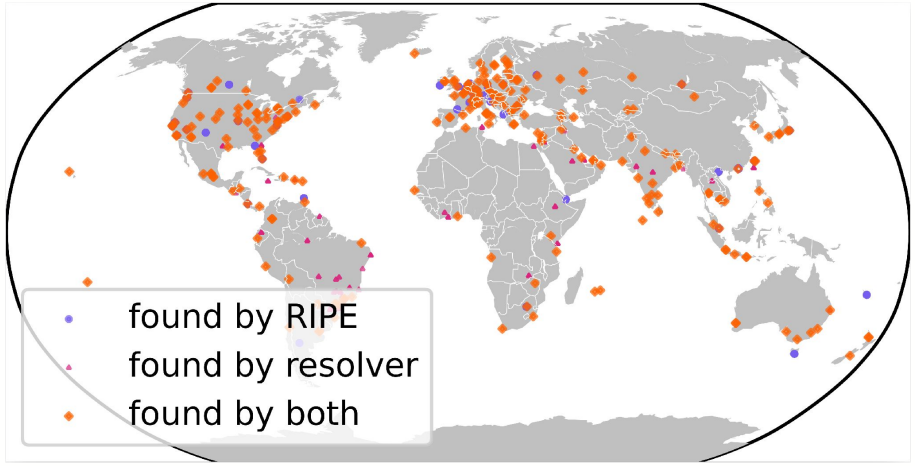
- Found **469 AS112 sites**, run by **97 operators**
  - 72 (2012) and 65 (2013) sites found in previous similar measurements
  - 40 operators are not on the self-reported “official” list
  - **Cloudflare**: 216 sites, queried by 41.71% of probes/resolvers
  - Resilience issue?



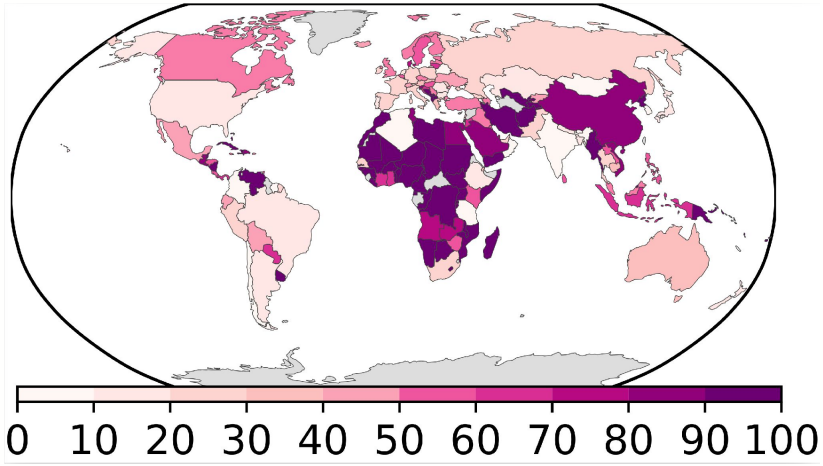


Where is AS112?

- Good coverage in **Europe, North America, Oceania**
- Some sites have very **large geographical reach**
- 32% of probes/resolvers sent queries across borders
- Only 8.47% of probes/resolver are in an AS that is connected to AS112
  - Only 5% query the site that they are connected to



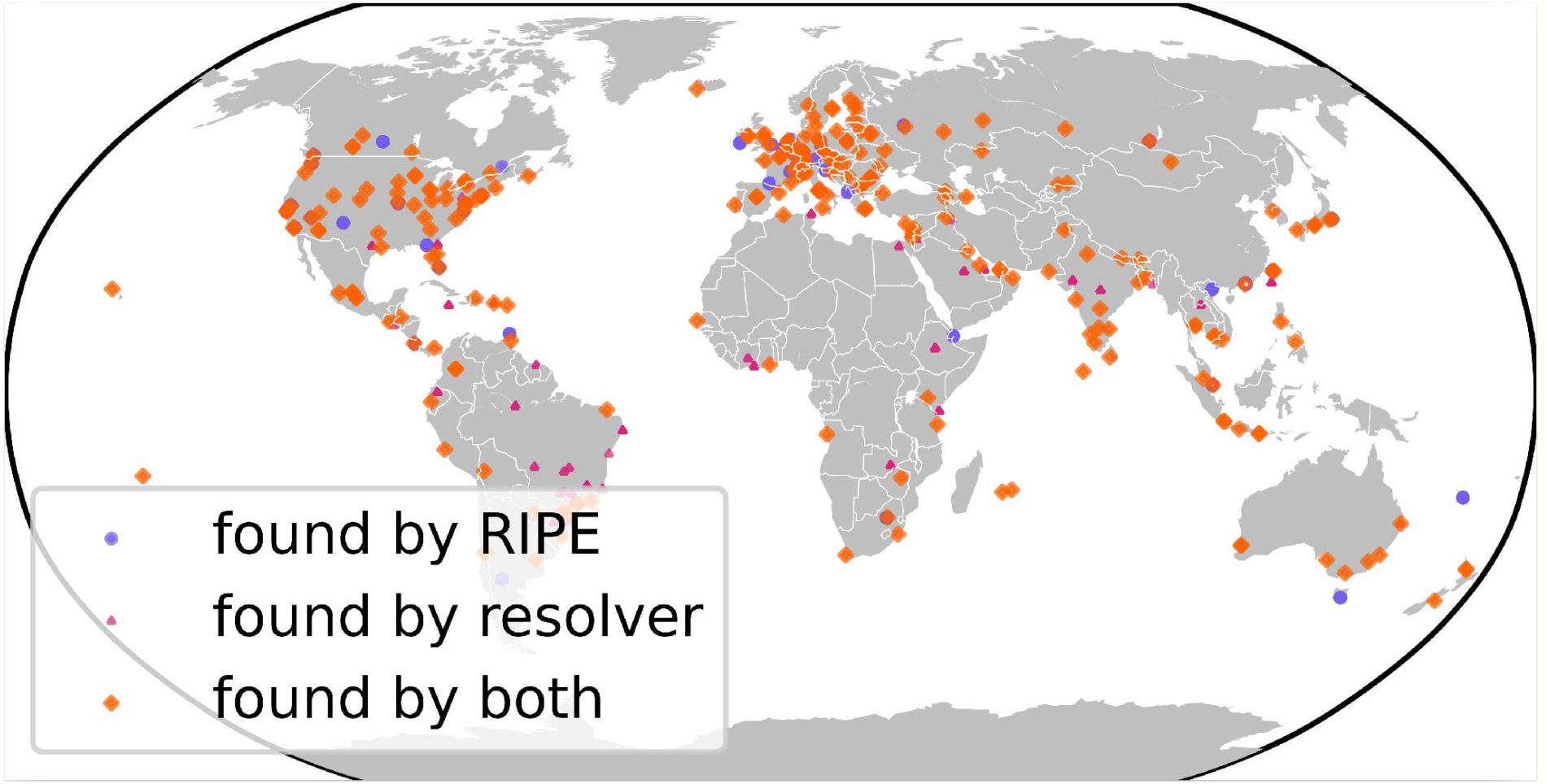
Location of AS112 sites



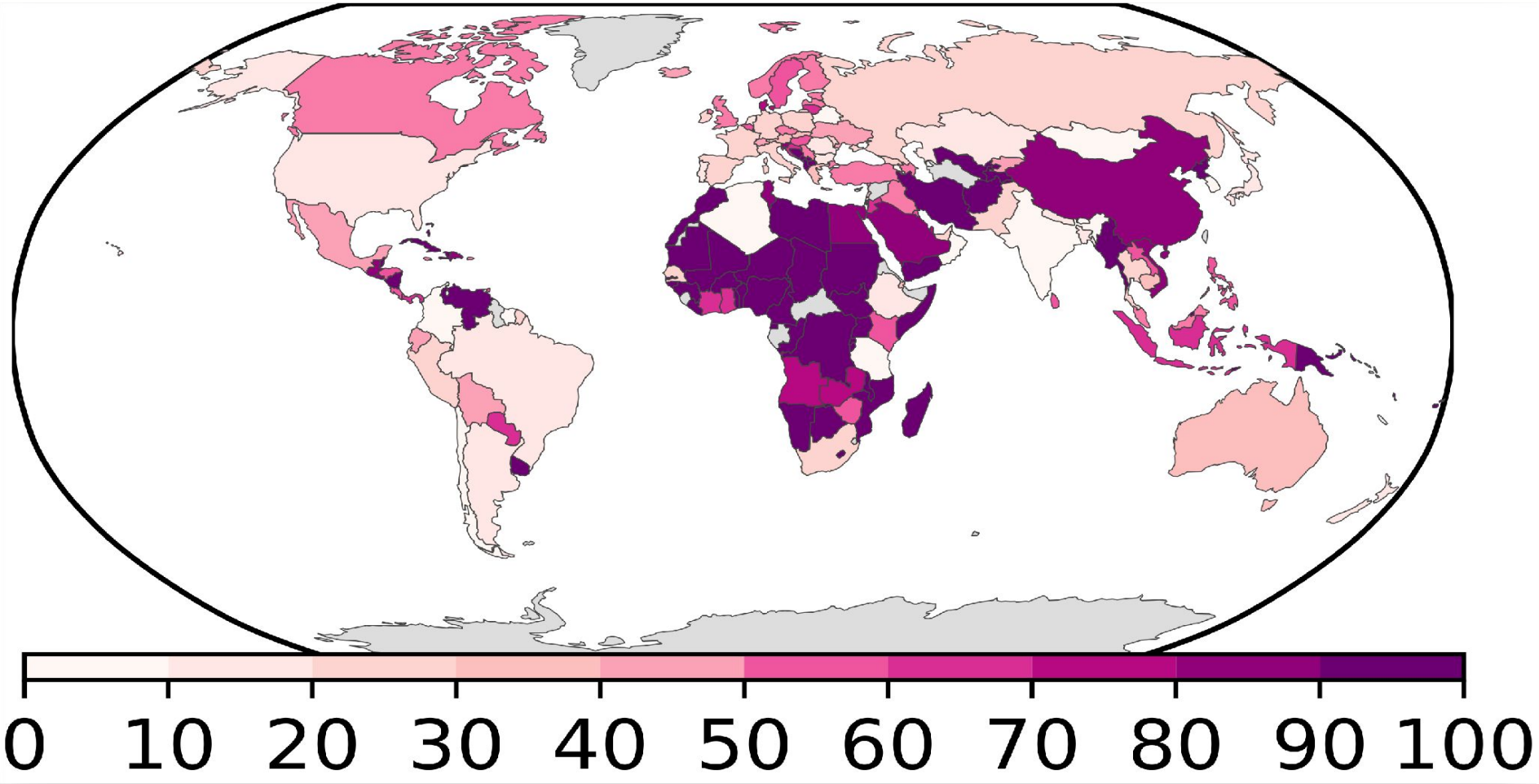
% queries sent to other countries

University of Glasgow

Where is AS112? (2)

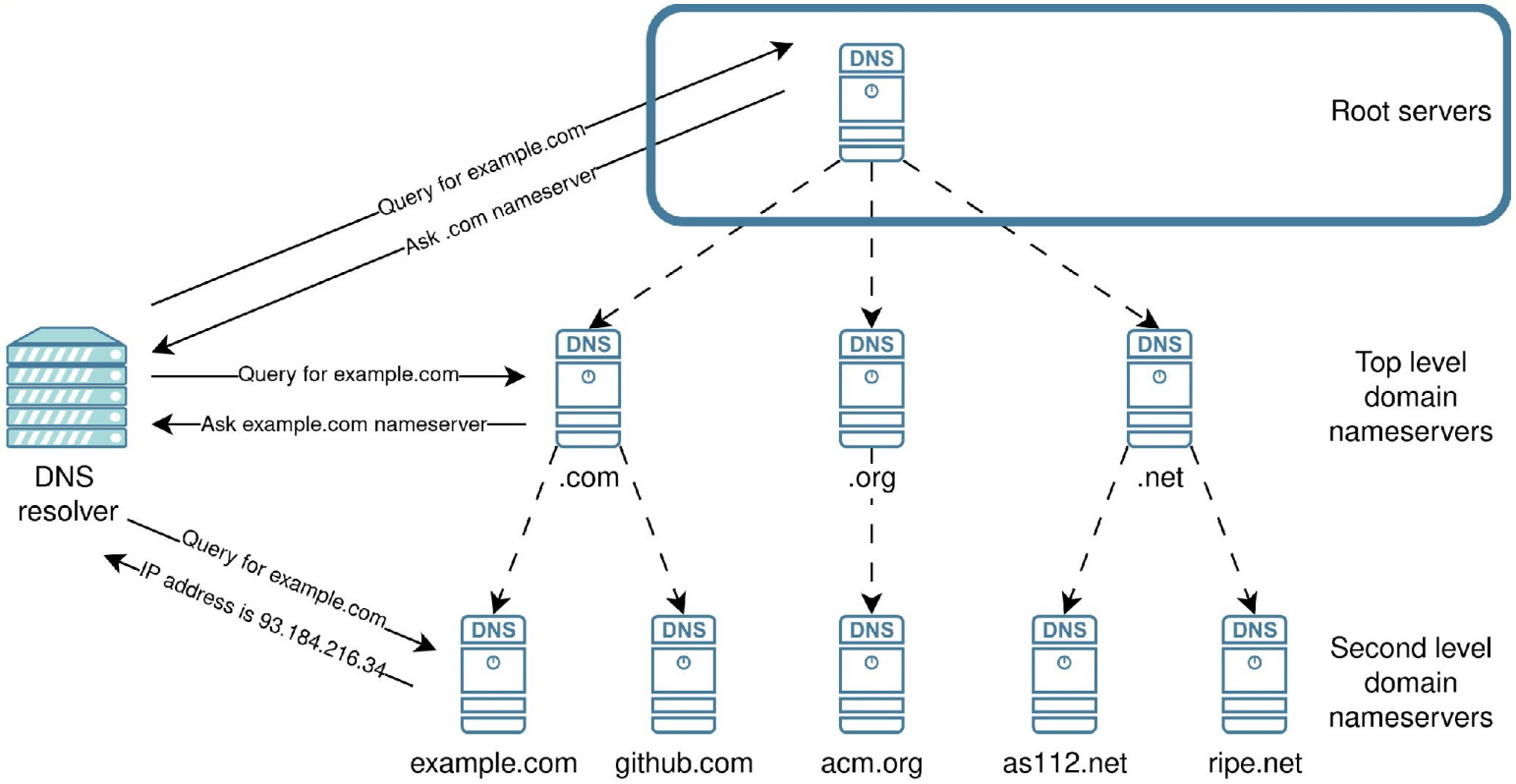


Where is AS112? (3)



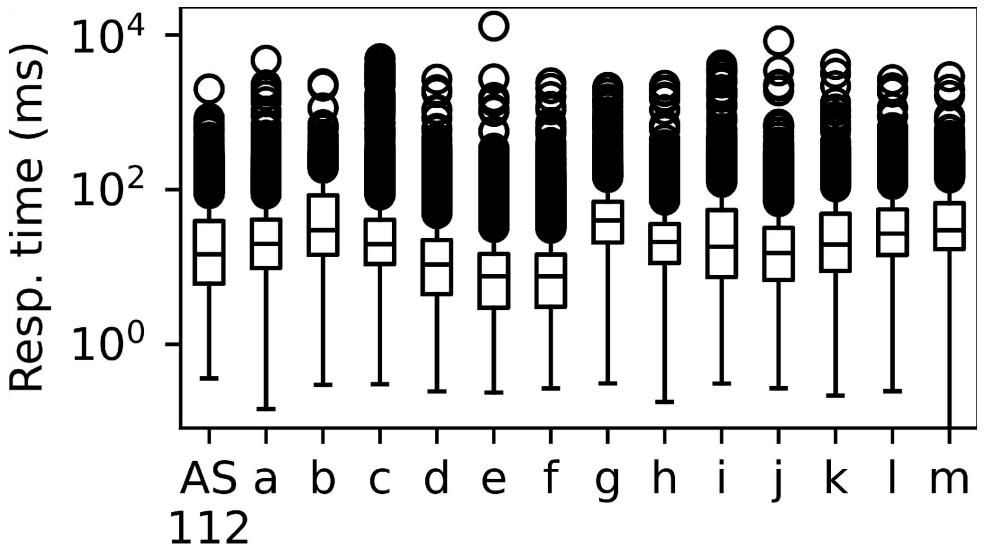
DNS Root Servers

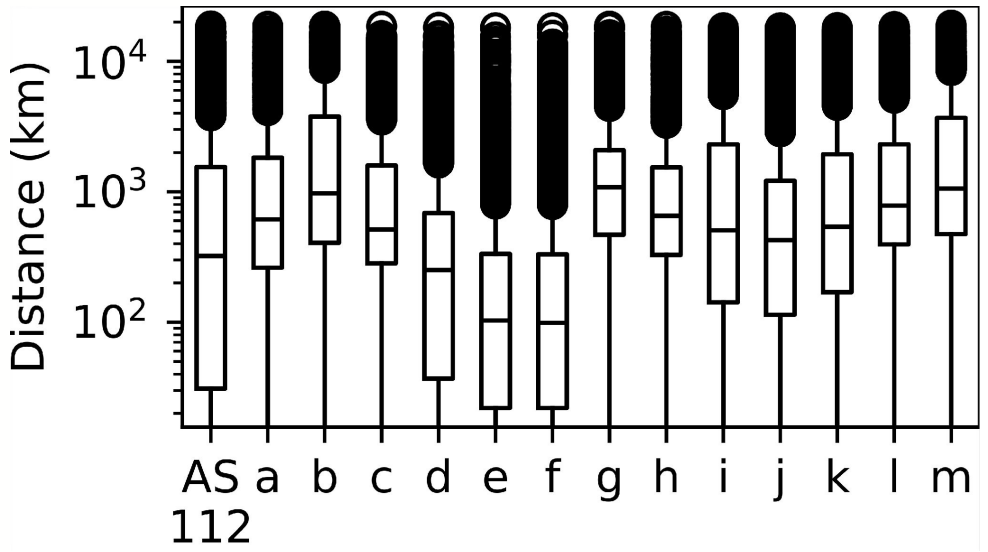
- Top of the DNS hierarchy, serve the root zone and .arpa
- 13 anycast networks (A-M root), run by 12 operators



AS112 vs DNS Root (1)

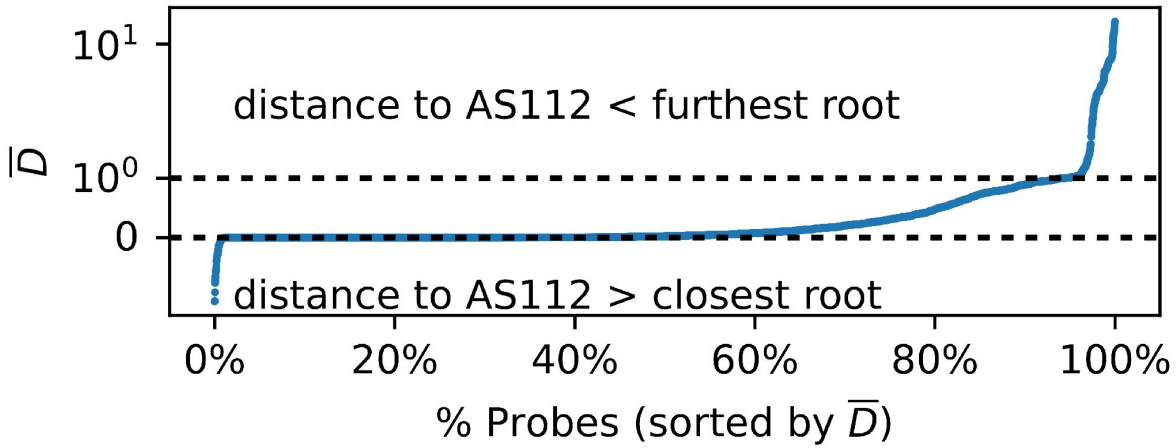
- Compared AS112 to DNS root servers
  - Can determine root server location with **`CHAOS TXT hostname.bind`** queries
- AS112 has 36.11% lower median distance, 23.21% lower median response time





AS112 vs DNS Root (2)

- For 22.65% of RIPE Atlas probes, distance to AS112 $\leq$ distance to the *closest* queried root site
- Distance to AS112 could be lower:
  - ~22% of probes/resolvers query the closest AS112 site (L-root: ~30%, B-root: ~83%)
  - Routing issues, local sites



University of Glasgow

- **Part 2: AS112 Privacy and Security**

- Our Dataset
- Reverse Mapping Queries
- Dynamic Updates
- Service Discovery
- Lame-Delegated Queries

University of Glasgow

What queries go to AS112?

- AS112 is volunteer-run and uncoordinated
- Relies on **assumption** that AS112 traffic is harmless
- Our questions:
  - **What queries** are sent to AS112?
  - What could a **malicious operator** do with these queries?
- **Work in progress**, these are preliminary results

Our Dataset

- DNS-OARC Day in The Life 2025 data (8-10 April 2025)
  - **RIPE NCC site (Amsterdam): ~**542M requests, ~246K clients
  - **WIDE site (Osaka):** 2,252M requests, ~145K clients
  - **TIX site (Dar es Salaam): ~**4M requests, ~2K clients
  - In total: **2,799,058,875 requests, 393,183 clients**
- We found:
  - Reverse DNS queries
  - DNS Dynamic updates
  - Service Discovery queries
  - Lame-delegated queries

RFC1918 Reverse Mapping Queries

- Most requests are for **reverse mappings of RFC1918 private addresses**
  - **37.62%** PTR (rDNS) queries for RFC1918 addresses
  - **27.09%** are other queries for RFC1918 reverse mappings (excluding service queries)
    - **33.8%** other query types (e.g. A, SOA, NS)
    - **50.04%** of form _.1.0.168.192.in-addr.arpa (due to QNAME minimisation)
    - Queries for personal devices, **9.69%** contain substring “iphone” (e.g., bobs-iphone.22.0.168.192.in-addr.arpa)

University of Glasgow

DNS Dynamic Updates

- DNS Dynamic updates change contents of zone, e.g. used by DHCP
- Sent to AS112 if:
  - Host uses private IP address, updates its reverse mapping
  - Local DNS doesn't serve the reverse mapping zone
- Studied in 2003 and 2006 [1,2]
- **5.80%** of requests are dynamic updates
  - Plus 0.57% TKEY queries to secure updates
- Malicious AS112 operator could learn local network configuration, and potentially track individual users

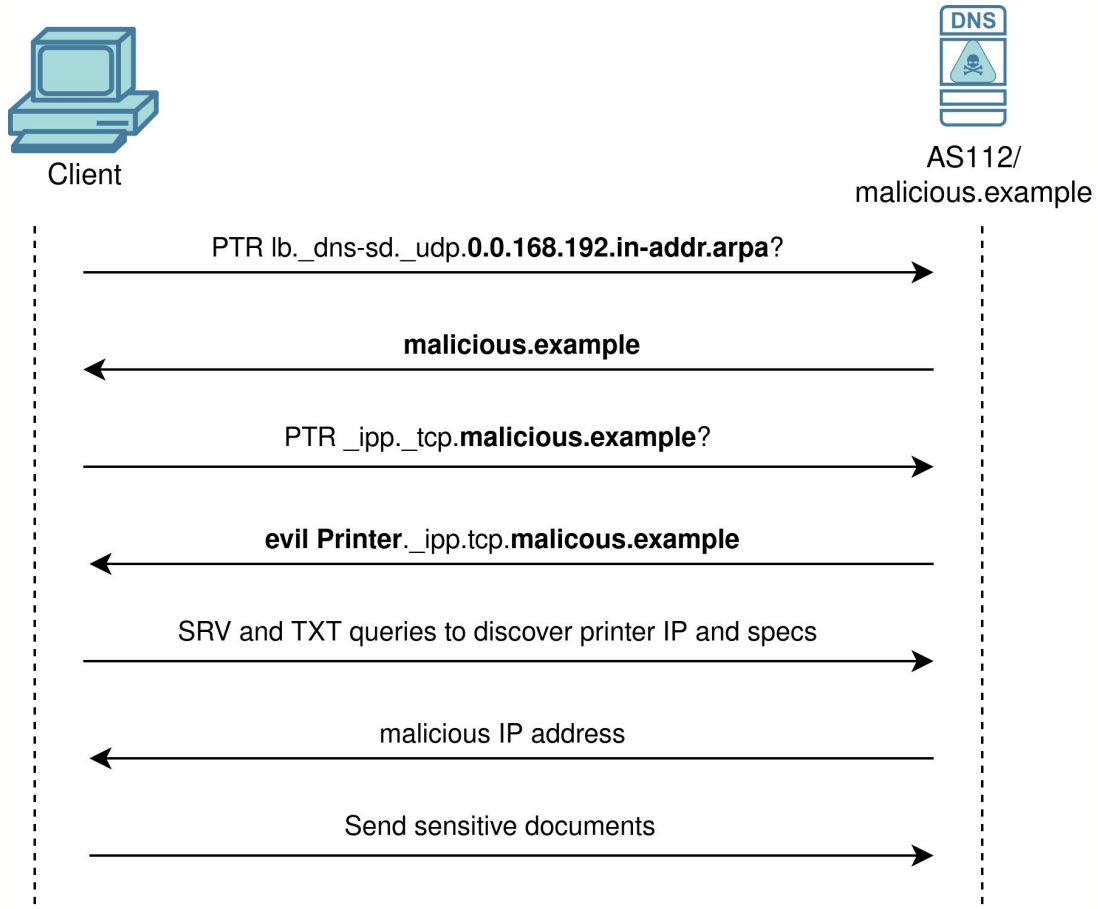
[1] Broido, A., Nemeth, E. and claffy, kc 2003. Spectroscopy of private DNS update sources. Proceedings the Third IEEE Workshop on Internet Applications. WIAPP 2003 (Jun. 2003), 19–29.
[2] Broido, A., Shang, H., Fomenkov, M., Hyun, Y. and Claffy, K.C. 2006. The Windows of Private DNS Updates. ACM SIGCOMM Computer Communication Review. 36, 3 (2006).

Service Discovery Queries (1/3)

- Interaction between AS112 and DNS-Based Service Discovery
  - Client discovers services by sending queries of the form
  - `_<service name>._<protocol>.`**`<local domain>`** to the local DNS
    - e.g. `_ipp._tcp.example.com`
  - Client has to first discover the **`<local domain>`**, through PTR queries of the form `lb._dns-sd._udp.`**`<bootstrap domain>`**
    - Process is called **Browsing Domain Discovery**
  - This bootstrap domain can be the **reverse mapping of the local address**
    - Queries go to AS112 if local address is RFC1918 private address, and local DNS does not serve this zone!

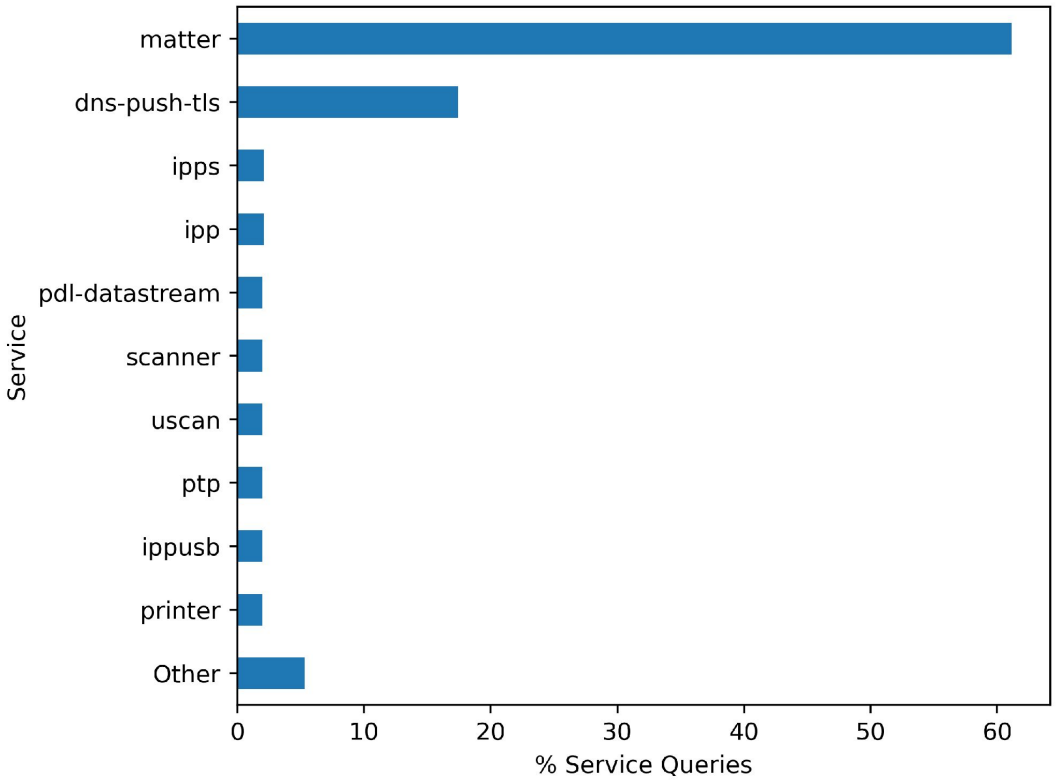
Service Discovery Queries (2/3)

- **18.17%** of requests are Browsing Domain Discovery queries
- Malicious operator could misuse these queries to spoof any service
  - Return a bogus local domain, then return bogus IP address for the service
  - Fails if service is authenticated



Service Discovery Queries (3/3)

- **6.71%** of requests contain a service name
  - 320 services
  - “matter” was the most common (61.13%)
- Can be used to spoof local services if service is not authenticated



University of Glasgow

Lame-delegated Queries

- 0.35% of requests are for domains not delegated to AS112, with public TLDs
- Malicious operator could respond and **spoof the site**
  - 38,447 domains; 43% of queries are for strepsils[.]top (malware/phishing domain!)
- Why are these queries going to AS112?
  - Historical zone files and WHOIS for ~20k domains (from VirusTotal and DNS Coffee)
    - ~95% were **delegated to AS112** in the zone files (lame delegation)
    - Of these, ~75% use the same registrar (Hosting Concepts B.V.), 24.90% contain “bet|poker|gambl|win|slot|casino|kasino”
- Has anyone heard of this?

University of Glasgow

Conclusions

- AS112 is widely deployed, similar/better than some root deployments
  - 469 sites, 97 operators
  - but coverage varies, resilience might be limited
- AS112 does not only receive “harmless” reverse DNS queries
  - Found dynamic updates, service queries, and lame-delegated queries

Elizabeth Boswell, University of Glasgow

e.boswell.2@research.gla.ac.uk

https://www.gla.ac.uk/pgrs/elizabethboswell/