Measuring Resilience of (Authoritative) DNS

Florian Steurer, Amreesh Phokeer, Philip Paeps, Liz Izhikevich

DNS Resilience

- Internet is increasingly hosting mission-critical applications and services
- Regulations such as NIS2 (EU) and CSF2 (US) to protect critical infrastructures
- We propose a two-step approach to measure authoritative DNS resilience at Internet-scale
  - We extract multiple resilience metrics based on the name servers (NSes) of a zone
  - We develop a new method to aggregate arbitrary metrics over the full dependency graph of a domain

Resilience metrics

- Measurable vs non-measurable practices
- Organizational processes are usually not measurable
- Focus on observable characteristics

How can resilience be measured?

- Resilience of zones depends on their parent zone and name servers, forming a **complex dependency graph**.
- We extract resilience metrics based on the **name servers** (direct dependencies) of a zone
- To account for **transitive dependencies**, we develop a **new method** to **aggregate arbitrary metrics** over the full dependency graph of a domain

Different measures for different threats

Metric	Resilience against	Dataset
# auth. NSes	node failures	active scans [5]
# IP addr. of auth Nses	node failures	active scans [5]
# of ASes of NS IP addr.	routing issues	PFX2AS [6]
# of anycast addresses	site failures, DDoS	MAnycast2 [4], IPInfo [7]
# of TLDs of NS names	NS parent zone failures	active scans [5]
# of server locations	site failures, geofencing	IPInfo Location [7]

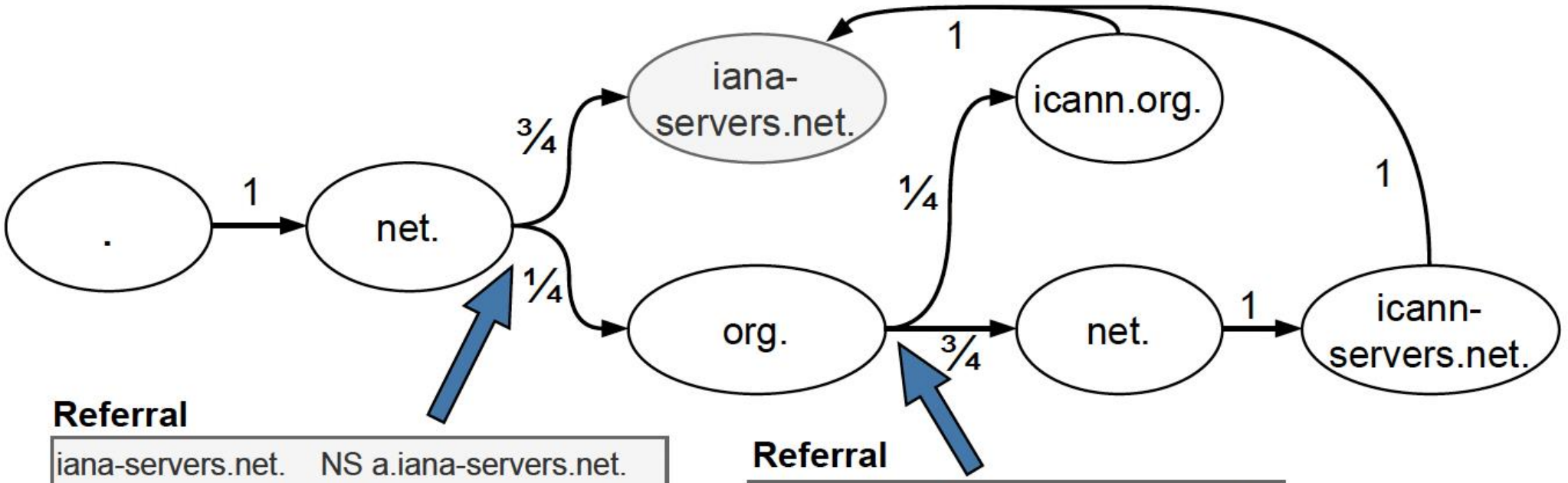
[4] Sommese et al., "MAnycast2: Using Anycast to Measure Anycast“, IMC, *2020*

[5] Steurer et al., "A Tree in a Tree: Measuring Biases of Partial DNS Tree Exploration “, PAM, *2025*

[6] CAIDA UCSD, RouteViews prefix2as dataset. https://www.caida.org/catalog/datasets/routeviews-prefix2as/, 2008

[7] IPInfo, *Trusted IP Data Provider from IPv6 to IPv4. https://ipinfo.io, 2025*

Resolution graph for iana-servers.net.



Transitive dependencies

- Resolvability of a zone relies on the resolvability of its parent zone and its NSes
- To quantify the influence of (transitive) dependencies, we propose to measure the *importance* of the dependency.
- To compute the importance score, we rely on enumerating possible resolution paths

Metric aggregation

- Model possible resolutions as a **weighted graph**
- Assuming uniform name server selection for edge weights
- Multiply weights along each path
- $importance_n(d)$ of dependency d for name n is the sum of weights over all paths where the dependency d occurs

Aggregate metrics over dependencies using the importance

$$M_{trans}(n) = \min_{d \in deps} (importance_n(d)^{-1} * M_{direct}(d))$$

Data Collection

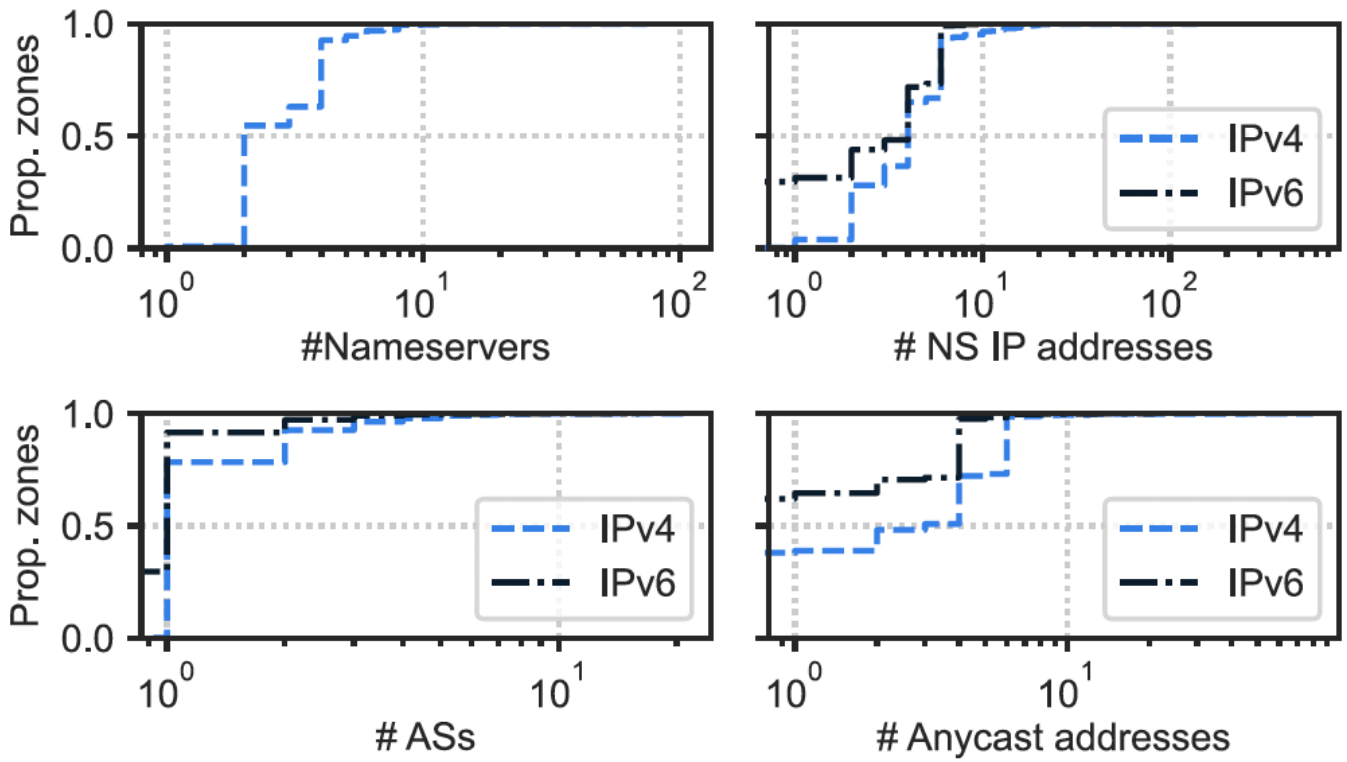
- ct: Names from unexpired certificates from Certificate Transparency logs: Argon, Xenon, Oak, Sectico Sabre, CloudFlare Nimbus, DigiCert Nessie, DigiCert Yeti, and TrustAsia.
- zf: Zone files from ICANN's Centralized Zone Data Service (CZDS) and available TLDs (.se, .nu, .ee, .ch, and .li).
- opendata: Names from the open-data efforts of AFNIC [2] and SK-NIC.
- Top-lists: Names from the corresponding domain top-list such as tranco, majestic, radar, umbrella:

Target list

		#Domains	#Unique to source	#Below SLD
By Source	ct	696,487,135	589,186,623	492,898,606
	zf	217,438,044	112,862,815	23,341
	opendata	4,626,781	2,489,116	72
	tranco	1,000,000	18,203	0
	majestic	1,000,000	45,760	921
	radar	1,000,488	18,169	345
	umbrella	1,000,000	602,276	790,167
Sum$_{bySource}$		922,552,448	705,222,962	493,509,151
By TLD	com	454,938,301	377,277,850	276,016,574
	net	41,284,999	36,081,396	26,418,624
	org	22,798,581	17,671,810	11,033,936
	de	17,569,119	17,522,361	10,866,642
	io	12,770,554	12,750,067	11,456,784
	uk	11,503,887	11,468,806	7,062,585
	ru	9,767,399	9,694,778	7,323,877
	rest	242,113,140	222,755,894	143,330,129
Sum$_{byTLD}$		812,745,980	705,222,962	493,509,151

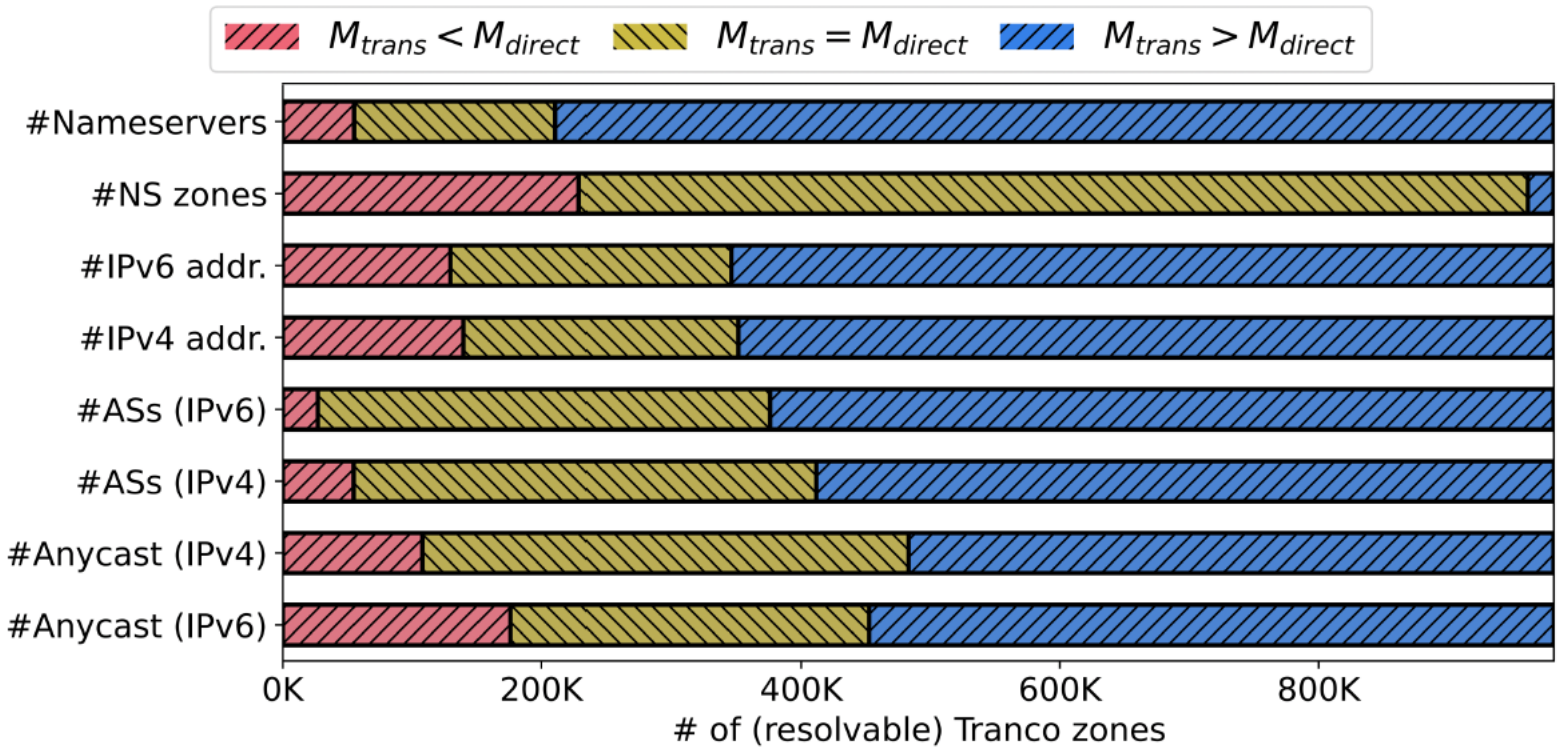
Direct metrics

- Resilience metrics for the Tranco Top 1M domains [2]
- IPv6 deployments include fewer addresses, ASes, and rely less on anycast



Transitive vs. direct metrics

- $M_{trans} < M_{direct}$ indicates that transitive dependencies may be **less resilient** than the zone itself.
- Potentially reduced resilience metrics for **5.6%** (#Nameservers) to **23.3%** (#NS zones) of zones



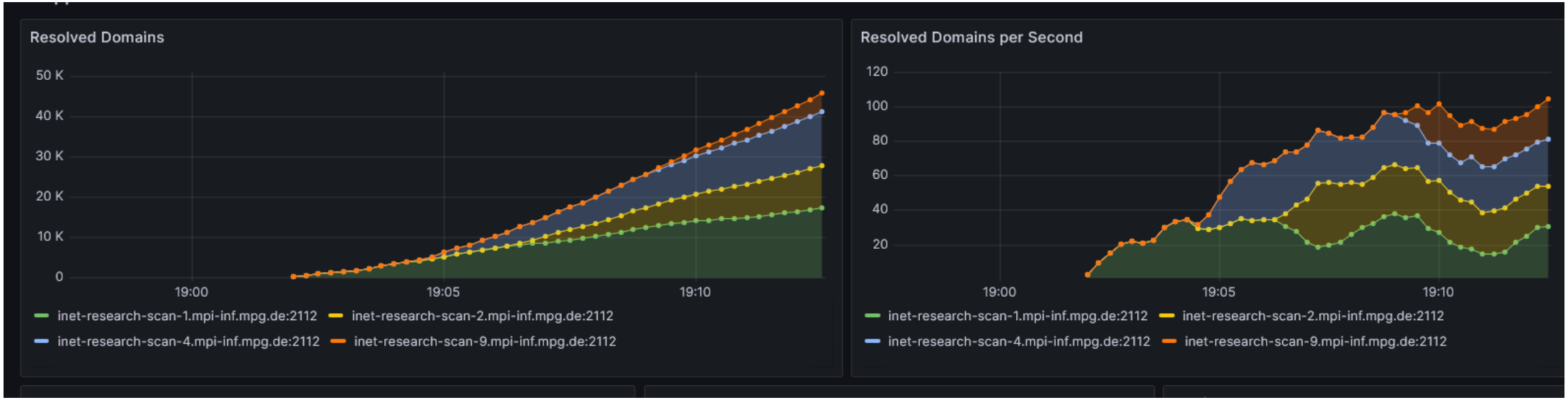
Tooling - YoDNS

YoDNS queries for DS, DNSKEY, CDS, CDNSKEY, CAA, TXT, MX, SOA, plus the TXT records

1 full scan is around 40 days

87 TB of DNS data covering 812M

Dashboard


Resolved Domains
50 K
40 K
30 K
20 K
10 K
0
19:00
19:05
19:10
inet-research-scan-1.mpi-inf.mpg.de:2112
inet-research-scan-2.mpi-inf.mpg.de:2112
inet-research-scan-4.mpi-inf.mpg.de:2112
inet-research-scan-9.mpi-inf.mpg.de:2112
Resolved Domains per Second
120
100
80
60
40
20
19:00
19:05
19:10
inet-research-scan-1.mpi-inf.mpg.de:2112
inet-research-scan-2.mpi-inf.mpg.de:2112
inet-research-scan-4.mpi-inf.mpg.de:2112
inet-research-scan-9.mpi-inf.mpg.de:2112

KINDNS Measurable practices **Authoritative Server operators**	**TLDs, SLDs and Critical Zones**
Practice 1 – DNSSEC and Key management	Covered
Practice 2 – Limited zone transfer	Covered
Practice 4 – Authoritative and recursive on different servers	Covered
Practice 5 – Two distinct name servers	Covered
Practice 6 – Software diversity / Network diversity / Geographic Diversity	Covered

Thank you