Poster: Observable KINDNS: Validating DNS Hygiene

Raffaele Sommese
University of Twente

Mattijs Jonker
University of Twente

KC Claffy
CAIDA/UCSD

CCS CONCEPTS

• **Networks → Naming and addressing**;

ACM Reference Format:
Raffaele Sommese, Mattijs Jonker, and KC Claffy. 2022. Poster: Observable KINDNS: Validating DNS Hygiene. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3517745.3563016

Introduction. The Internet's naming system (DNS) is a hierarchically structured database, with hundreds of millions of domains in a radically distributed management architecture. The distributed nature of the DNS is the primary factor that allowed it to scale to its current size, but it also brings security and stability risks. The Internet standards community (IETF) has published several operational best practices to improve DNS resilience, but operators must make their own decisions that tradeoff security, cost, and complexity. Since these decisions can impact the security of billions of Internet users, recently ICANN has proposed an initiative to codify best practices into a set of global norms to improve security: the *Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS)* [4]. A similar effort for routing security – Mutually Agreed Norms for Routing Security – provided inspiration for this effort. The MANRS program encourages operators to voluntarily commit to a set of practices that will improve collective routing security – a challenge when incentives to conform with these practices does not generate a clear return on investment for operators. One challenge for both initiatives is independent verification of conformance with the practices. The KINDNS conversation has just started, and stakeholders are still debating what should be in the set of practices. At this early stage, we analyze possible best practices in terms of their *measurability* by third parties, including a review of DNS measurement studies and available data sets (Table 1).

IMC '22, October 25–27, 2022, Nice, France

ACM ISBN 978-1-4503-9259-4/22/10…$15.00
https://doi.org/10.1145/3517745.3563016

Proposed practices for KINDNS. The KINDNS group has proposed practices (**P**) specific to authoritative (**A**) and recursive (**R**) nameservers, and those for general hardening (**H**) of infrastructure. We focus our analysis on public-facing DNS infrastructure: open resolvers and authoritative nameservers. We identify practices that are not measurable and suggest practices based on previous scientific studies. Table 2 uses ICANN's current numbering of KINDNS practices [4].

Measurable Practices. Table 2 lists practices that are at least somewhat amenable to third-party measurement, based on existing literature. For each practice, we identify the main goal, data required for independent validation, relevant measurement tools, and additional notes. We note caveats with measurement of some practices. For example, verifying that a server is not hosting both recursive resolution and an authoritative zone. `A7-b` requires precise geolocation accuracy (e.g., .identifying servers in the same rack), not generally possible with current tools. `A2,A6,H1-a` are limited by ethical implication of scanning.

Not Measurable Practices. Some proposed practices are not amenable to third-party verification due to lack of available data or lack of access to *internal* vantage points: `A-P8|R-P6: Monitoring`, `R-P2 Allow internal traffic only`, `H-P7: SSH authentication`, and `H-P3-P4-P5: Server hardening, integrity, and versioning`.

For some proposed practices, we identify datasets that may offer a path forward. For example, to measure `A-P3: Zone Integrity`, one could leverage a rapid zone update service (a live stream of zone changes) such as once offered by Verisign. This data would help researchers study zone integrity impairment events (e.g., .DNS hijacking), but requires that TLD registries be willing to share that data.

Missing Measurable Practice. **Anycast deployments for critical zones**: Several studies [5, 6] have demonstrated the value of anycast deployments of critical DNS infrastructure to increase the DNS resilience against DDoS attacks. Anycast is a de-facto standard with peaks of 97% of TLDs [10].

DNS Provider diversity: The Dyn 2016 incident and previous studies [2, 10] illustrated the importance of relying on different providers (ASN) for increase DNS resilience.

Caching Best Practice: Long TTL values for DNS infrastructure records increase resilience against DDoS attacks [7].

Prevent inconsistent and lame delegations to mitigate risk of domain hijacking, especially for critical zones. Researchers have found this vulnerability has affected multiple TLDs and prominent SLDs [1, 9].

Table 1: Datasets available to enable independent verification of DNS hygiene practices.

Index	Scan Type	Example	Data Contained	Limitation	Frequency	Accessibilty
1	Active DNS Scan	OpenINTEL Rapid7 FDNS	Full DNS Record Scan (OI) A/AAAA/MX/NS (R7)	Coverage (≈ 60% of Namespace)	Daily(OI) Weekly(R7)	Limited OpenData (OI) Under Agreement(R7)
2	Port Scan	Rapid7 Sonar port scans	Port Scan of common UDP/TCP service	IP banning - Not covering all ports	Weekly	Under Agreement
3	OpenResolver Census	Shadowserver Yazdani et al. .[11]	List of public exposed openresolvers	No visibility on private resolvers	Weekly	Under Agreement
4	DNS traffic samples	OARC DITL	Traffic Sample from several root server sand TLDs	Root-specific view Anonymization	24 hrs/year	OARC Membership
5	DNS traffic streams	Domain Tools SIE	Passive DNS Data	Coverage	Continuously	Limited OpenData Commercial
6	DNS databases	Domain Tools DNSDB	DNS Meta-Data	Coverage	Continuously	Limited OpenData Commercial
7	Zone Archive	DZDB OARC Zone Archive	Archive of Zone File	Limited mainly to CZDS zones	Daily (DZDB)	OpenData (DZDB) OARC Membership
8	MANRS compliance	Spoofer Data BGPStream/GRIP	RPKI/BCP38 compliance	Spoofer: Limited to participating actors	Variable	Limited OpenData
9	Geolocation	NetAcuity, Maxmind OpenIPmaps, Hoiho	IP Geolocation	Limited Accuracy	Variable	Under Agreement

Table 2: Feasibility of independent verification of KINDNS Practices. Data sources from Table 1.

#	Practice Description	Main Goal	Data for Indep. Verification	Relevant Tools	Notes
A-1	DNSSEC compliance, including key management	DNS response integrity	#1: Active Daily Scan	dnsviz, Zonemaster hardenize.com	Previous Study: [8]
A-4|R-4	Authoritative and Recursive DNS software not on same server	Mitigate DoS attack risks	#1: Active Daily Infra Scan (OpenINTEL) joined with #3: OpenResolvers Census	dig (A-4)	Limited coverage
A-5	Multiple authoritative nameserver per zone	Redundancy for resilience Avoid Single Point of Failure	#1: Active Daily Infra Scan (OpenINTEL)	Zonemaster Methods:[2, 10]	Weak metric; Provider diversity can improve it
A-7a	Topological Diversity		#1: Active Daily Infra Scan (OpenINTEL) + Prefix2AS	Zonemaster hardenize.com	Prefix vs AS granularity. Previous study: [10]
A-7b	Geographical Diversity		#1: Active Daily Infra Scan (OpenINTEL) + #9: Geolocation	geolocation tools + dig	Limited accuracy and precision of dataset
A-2	Zone Transfer Restricted	Prevent Leak of Zone Files	AFRX Scan of NS IPs #1 Active Daily Infra Scan (OpenINTEL)	dig	Ethics and Privacy concerns
A-6|R-7	Software Diversity	DNS Software resilience	Fingerprinting of NS IPs #1 Active Daily Infra Scan (OpenINTEL)	dig	Ethics concerns Hard to Measure
R-1	DNSSEC Validation	DNS response integrity	Active Scan of #3 Open Resolvers IP lists	dig CheckMyDNS	Cf. Signing (A-1 compliance)
R-3	QNAME Minimization	User privacy of Queries	#4 DNS Traffic Samples #5 DNS Traffic Streams	Manually check resolver config.	Previous study: [3]
H-1a H6	ACL: Allow DNS Traffic Only; Management Access Restricted	Reduce Attack Surface	#2 Port Scan Census	nmap	Limited coverage using available census
H-2a	BCP38	Prevent Spoofing	#8 Spoofer data	spoofer.caida.org	Prevents amplification
H-2b	MANRS	Prevent Hijacking	#8 MANRS compliance data	Checking route/ACL configuration	
H-8	2FA Customer Access	Prevent Hijacking	N/A	Manually	Require manual registration to provider portal

Conclusion. At this early stage of the KINDNS initiative, we encourage ICANN to consider the set of practices from a transparency and accountability perspective. Existing projects such as OpenINTEL go a long way toward supporting independent verification of some practices, often in collaboration with registries. For other practices, conformance verification will require operators to provide access to more data. This tension is consistent with the intense debates over managing trusted access to registration data due to GDPR. We believe the academic community could meaningfully contribute to this conversation by analyzing proposed practices from a measurement perspective.

Acknowledgements. This work is based on research sponsored by NWO-DHS MADDVIPR project (628.001.031/FA8750-19-2-0004), the EU CONCORDIA project (830927) the U.S. NSF grants OAC-2131987 and OAC-1724853. The views and conclusions are those of the authors and do not necessarily represent endorsements, either expressed or implied, of the sponsors.

[1] G. Akiwate et al. 2020. Unresolved Issues: Prevalence, Persistence, and Perils of Lame Delegations *(IMC '20)*.
[2] M. Allman. 2018. Comments on DNS Robustness *(IMC '18)*.
[3] W.B. de Vries et al. 2019. A First Look at QNAME Minimization in the Domain Name System *(PAM '19)*.
[4] ICANN. 2022. KINDNS. (2022). https://kindns.org/
[5] G.C.M. Moura et al. 2016. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event *(IMC '16)*.
[6] G.C.M. Moura et al. 2018. When the Dike Breaks: Dissecting DNS Defenses During DDoS *(IMC '18)*.
[7] Giovane C. M. Moura et al. 2019. Cache Me If You Can: Effects of DNS Time-to-Live *(IMC '19)*.
[8] M. Muller et al. 2020. The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle *(IMC '20)*.
[9] R. Sommese et al. 2020. When parents and children disagree: Diving into DNS delegation inconsistency *(IMC '20)*.
[10] R. Sommese et al. 2021. Characterization of Anycast Adoption in the DNS Authoritative Infrastructure *(TMA '21)*.
[11] R. Yazdani et al. 2022. A Matter of Degree: Characterizing the Amplification Power of Open DNS Resolvers *(PAM '22)*.