

Observable KINDNS

Validating DNS Hygiene

Raffaele Sommese¹, Mattijs Jonker¹, KC Claffy²
University of Twente¹, CAIDA/UC San Diego²

Introduction

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). We analyzed possible best practices in terms of their measurability by third parties with available and collectible datasets.

Datasets and Practices

Goal	Practice	Measurable	Datasets"
DNS Response Integrity	DNSSEC compliance; Key management	✓	Active DNS Scan
Mitigate DoS attack risks	Authoritative and Recursive DNS software not on the same server	⚠ *	Active DNS Scan OpenResolvers Census
Redundancy for Resilience Avoid Single Point of Failure	1. Multiple Authoritative Nameservers per Zone 2. Topological Diversity 3. Geographical Diversity	⚠ *	Active DNS Scan Prefix2As Geolocation
Prevent Leak of Zone Files	Zone Transfer Restricted	⚠ **	AFRX Scan of NS IPs from Active DNS Scan
DNS Software Resilience	Software Diversity	⚠ **	Fingerprinting of NS IPs from Active DNS Scan
DNS Client Response Integrity	DNSSEC Validation	✓	Active Scan of OpenResolvers IP lists
Users Privacy	QNAME Minimization	✓	DNS Traffic Samples DNS Traffic Streams
Reduce Attack Surface	ACL: Allow DNS Traffic Only Management Access Restricted	⚠ **	Port Scan Census
Prevent Spoofing/Hijacking	BCP38/MANRS	✓	Spoofers, MANRS data
Prevent Hijacking	2FA Authentication	✓	Manual Inspection
Prevent Hijacking	Zone Integrity	✗	Rapid Zone Update Required
Internal Hardening	Monitoring, ACLs, SSH Keys Policies	✗	Internal VPs Required

* Limited Visibility, **Ethics Concern

"For more details on available datasets, check our extended abstract

How can researchers help?

- 1) Identify missing practices: (i) Anycast deployments for critical zones; (ii) DNS Provider diversity; (iii) Caching Best Practices; and (iv) Prevent inconsistent and lame delegation
- 2) Shape a framework for responsible data sharing of DNS and complementary datasets between industry and independent researchers.
- 3) Assess the adoption of KINDNS best practices via large-scale measurement studies.

KINDNS



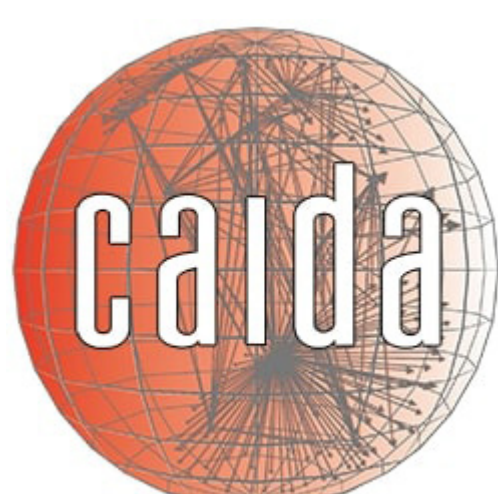
Interested? Contact us for collaboration!

r.sommese@utwente.nl
m.jonker@utwente.nl
kc@caida.org

Abstract



UNIVERSITY
OF TWENTE.



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.

