Observable KINDNS: Validating DNS Hygiene

Raffaele Sommese[1], Mattijs Jonker[1], KC Claffy[2]

[1] University of Twente, [2] CAIDA/UC San Diego

OARC 39, 22–23 Oct 2022, Belgrade, Serbia

Introduction

- Several best practices to improve DNS resilience have appeared in RFCs, but operators must make their own decisions that tradeoff security, cost, and complexity.
- These decisions impact the security of billions of Internet users.
- 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)***.

KINDNS: a MANRS for DNS

- Inspired by similar effort for improving routing security: **Mutually Agreed Norms for Routing Security (MANRS)**.
- The MANRS program encourages operators to voluntarily commit to a set of practices that will improve collective routing security.
- Many operators have joined the MANRS community.

Our Contribution

- One challenge for both initiatives: *independent verification of conformance with the practices*
- To address this challenge for KINDNS, we analyzed possible best practices in terms of **measurability** by third party.
- We leveraged previous academic research and currently publicly available datasets.

Categorizing KINDNS Practices

- The KINDNS group has proposed practices (P) specific to authoritative (A) and recursive (R) nameservers, and those for general hardening (H) of the infrastructure.
- We focus our analysis on public-facing DNS infrastructure: open resolvers and authoritative nameservers.
- We identify practices that are measurable (vs. not) and suggest additional practices based on previous scientific studies.

Authoritative Best Practices

Measurable Practice Summary

Goal	Practice	Measurability	Dataset	Tools
DNS Response Integrity	DNSSEC Enabled Authoritative	Yes	Active DNS Scan (e.g OpenINTEL)	Dnzviz, Zonemaster, hardenize.com
Increase Resilience Avoid SPoF	Geographically, Topologically, NS Diversity	Yes	Active DNS Scan, Prefix2AS, Geolocation	Zonemaster, Dig, Geolocation
Prevent Leak of Zone Files	Zone Transfer Restricted	**Maybe** Ethics Concerns	AFRX of Active DNS Scan	dig
Prevent Hijacking	2FA customer access	Yes	Manual	Manual

Recursive Best Practices

Measurable Practice Summary

Goal	Practice	Measurability	Dataset	Tools
DNS Response Integrity	DNSSEC Enabled Recursive	Yes Not Measured currently	OpenResolvers Scan	Dig
Improve User Privacy	QNAME minimization	Not Fully	DITL Traces	N/A

Common Best Practices

Measurable Practice Summary

Goal	Practice	Measurability	Dataset	Tools
Mitigate DoS attack risks	Authoritative and Recursive DNS software not on the same server	Limited Coverage	Active DNS Scan OpenResolvers Scan	Dig
DNS Software resilience	Software Diversity	Limited Not currently measured	Fingerprint DNS Servers	Nmap, dig
Reduce Attack Surface	ACLs	**Maybe** Ethics Concerns	Port scan census	nmap
Prevent Spoofing/ Hijacking	MANRS/BCP38	Yes	Spoofer MANRS Data	N/A

Non-Measurable Practices

Some proposedpractices are not measurable without an internal vantage point:

- Monitoring
- Internal ACL
- SSH Authentication requirements
- Server hardening, integrity and versioning

Others, like Zone Integrity (Authoritative, require sharing of **rapid zone updates.**

Missing Practices?

Anycast deployments for critical zones.

Caching Best Practice (e.g., Long TTL values for DNS infrastructure records increase resilience against DDoS attacks).

Prevent inconsistent and lame delegations by checking parent and children's zones.

Discussion

- Adopting best operational practices represents a fundamental pillar in improving DNS ecosystem resilience and security.
- If there is interest in third-party independent validation of conformance to best practices, it likely changes which practices to include.
- Our goal is to understand the measurability of these and other proposed practices.

Conclusion

- Assessing KINDNS best-practice requires a strong collaboration between different stakeholders.
- Independent researchers, ICANN and operators can work in synergy and share knowledge and data to improve DNS ecosystem security.
- Data and Knowledge sharing represent the key to achieving this goal.
- Some practices are already amenable to independent assessment.

Discussion Questions

- How can researchers help to assess conformance with DNS best practices?
- What do you think is missing?
- Are there ways to overcome concerns with data sharing?

Thanks for the attention

If you want to reach me:

r.sommese@utwente.nl

https://academia.r4ffy.info

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.