How to measure KINDNS?

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

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

DINR 2023

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.

What's measurable (and already measured)?

- DNSSEC Adoption (Active Scans, e.g., OpenINTEL, Rapid7)
- Geographically, Topologically, NS Diversity (Active Scans)
- QNAME minimization (Passive and Active Scans)
- MANRS/BCP38 compliancy (Spoofer)

What's still to measure?

- Authoritative and Recursive DNS software not on the same server
  - Focus on Open Resolvers
- ACLs and non-DNS service exposure (Port Scans)
  - Focus on well-known ports
- DoH/DoT adoption in the wild
- Software Diversity (Fingerprinting)
  - Challenging

Some (very) initial results

- Over 638K authoritative nameservers IPs :
  - 52% have web port (80) open
  - ~40% have mail ports open (25, 995, etc.).
  - 31% have SSH port open
  - Other popular ports open are: (s)FTP, Windows Share, SUN RPC
  - 1.5% of authoritative are recursion enabled!

Some (very) initial results

- Over 1613K recursive resolvers IPs:
  - 8% have web port (80) open
  - 6% have SSH port open
  - 5% have Telnet port open!!
  - We also see mail and other services
  - Only 85 DoH properly configured recursive resolvers and 78 DoT (currently investigating)

Non-Measurable Practices

Some proposed practices are not measurable without an internal vantage point:

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

AXFR scan (ethics?)

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

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 help reach me:

r.sommese@utwente.nl

https://academia.r4ffy.info

This work is based on research sponsored by NWODHS 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.

caida

UNIVERSITY
OF TWENTE.

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security

NWO
Netherlands Organisation
for Scientific Research