SWITS Abstract 2024

Fingerprinting DNS Resolvers using Query Patterns from QNAME Minimization

Jonathan Magnusson
Karlstad University
jonathan.magnusson@kau.se

May 12, 2024

1 Abstract

The Domain Name System (DNS) plays a pivotal role in the function of the Internet, but if the DNS resolvers are not correctly configured or updated, they could pose security and privacy risks. Fingerprinting resolvers helps the analysis of the DNS ecosystem and can reveal outdated software and misconfigurations. This study aims to evaluate if patterns in queries from DNS resolvers—implementing query name minimization as a privacy enhancing feature—can reveal their characteristics such as their software and versions. We examined the query patterns of minimizing resolvers at the authoritative name server side, and our findings indicate that distinct patterns correlate with specific open-source resolver software versions. Notably, none of the resolvers fully follow the recommended query name minimization algorithm outlined in RFC 9156, suggesting a discrepancy between recommendations and real-world implementations. We also identified high rates of query amplification, possibly caused in part by the combination of minimization and forwarding configurations. Our research contributes to understanding the current state of the DNS ecosystem, highlighting the potential for fingerprinting to enhance Internet security by identifying and addressing resolver-related risks.