Cost-aware Internet Security Decision Model

Enock Mbewe • Supervised By: Dr. Josiah Chavula •{embewe,jchavula}@cs.uct.ac.za

SCHOOL OF IT

Department of Computer Science

Project Description

This study aims to investigate the use of a security decision model to allow users to easily configure cost-aware security options that can map to complex Internet security mechanisms to achieve Confidentiality, Integrity, Authentication and Privacy (CIAP). Furthermore, this study investigates a decentralised internet security configuration framework to enable users to decide on the appropriate security level based on acceptable performance and privacy costs.

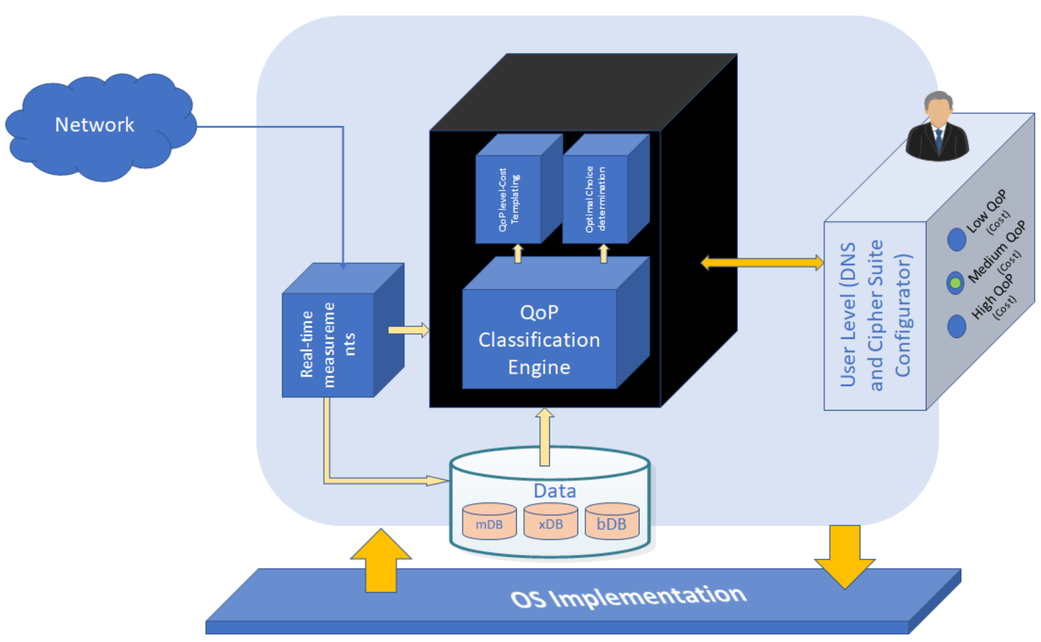
Motivation

(a) Increased Internet userbase $\Longrightarrow$ Increased cybercrimes
(b) So many complex security features not easily understood by average to novice Internet users.
(c) Internet security decisions centralised and hidden from users.

Research Questions

(a) What is the cost of integrated secure DNS and TLS cipher suites on the Quality of Internet browsing experience?
(b) What security and security design attributes should be considered to develop a security-performance classification model that maps to high-level user choices?
(c) How would a cost-aware security configuration framework impact users' Quality of Internet browsing Experience?
(d) How would a cost-aware security configuration framework impact users' adoption of Internet security mechanisms?

Conceptual Framework



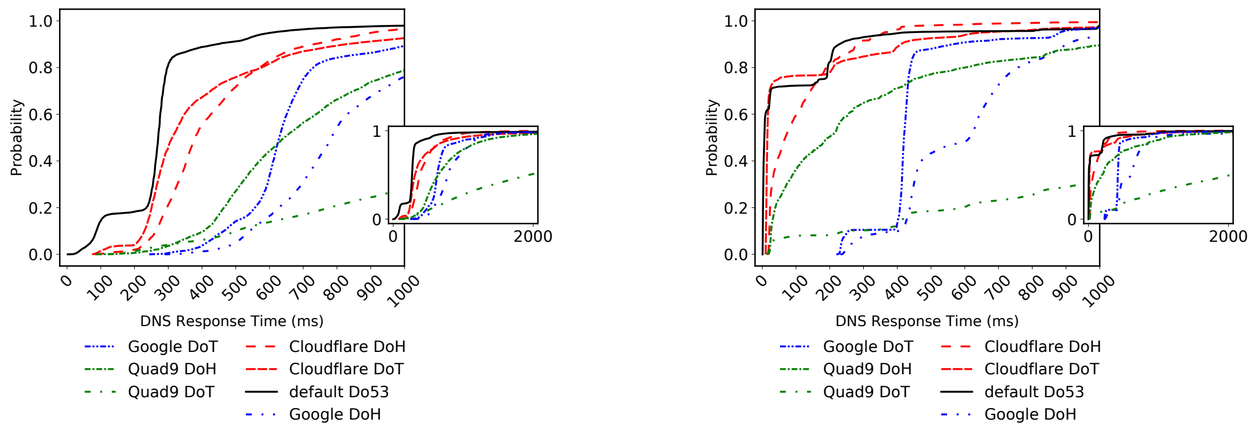
Research Contributions

(a) A specification method for combining different security configurations with a high-level system interaction model
(b) A framework for building Internet Quality of Protection tools for security protocols which have complex configuration structures.
(c) Adaptive integrated security-cost modelling based on empirical data

Research Approach

(a) Internet security measurements and lab experiments
(b) Generative and evaluative artefact user studies

Findings- Question 1



(a) DNS response time under 4G

(b) DNS response time under Campus Network

Figure 1. DNS timings for local Do53 vs Encrypted DNS from major DNS providers (Google, Cloudflare and Quad9) under 4G and Campus network

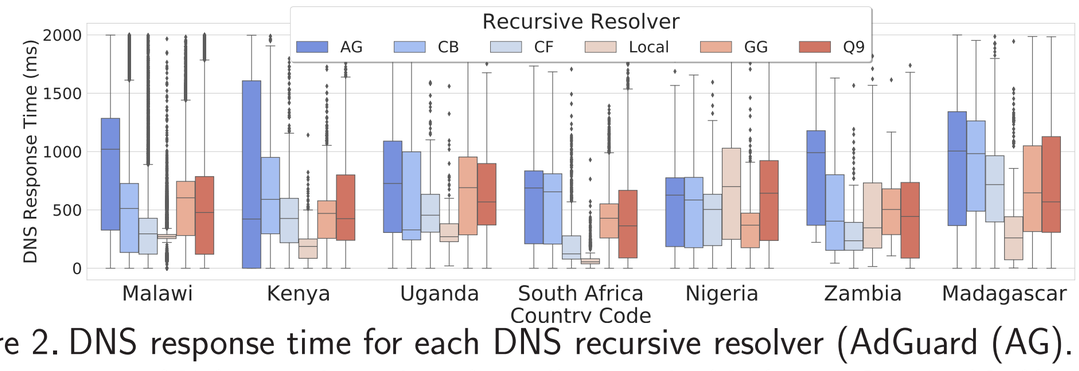


Figure 2. DNS response time for each DNS recursive resolver (AdGuard (AG). CleanBrowsing (CB), Local resolver (Local), Google (GG) and Quad9 (Q9)) across the vantage coutries under 4G

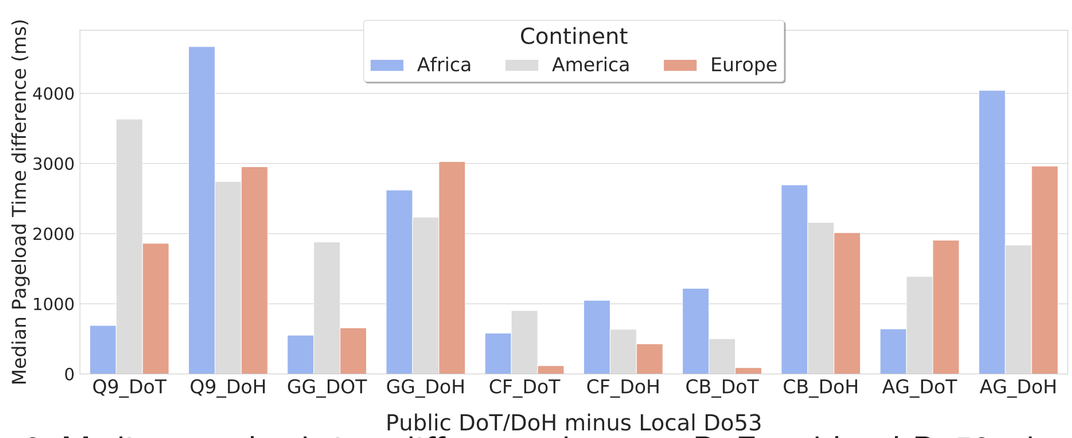


Figure 3. Median pageload time differences between DoE and local Do53 when resolving websites hosted in Africa, North America and Europe measured from 4G networks

Futute Work

(a) Currently doing a pre-design user study for Question 2
(b) Model design and evaluation - 2021
(c) Lab Experiments and evaluative user study - 2021

Acknowledgements

This research is financially supported by the Hasso Plattner Institute for Digital Engineering, through the HPI Research School at the University of Cape Town.

SCHOOL OF IT ICT4D HPI