

Project Description

In this research, we investigate the use of a cost-aware security decision model and a personal Internet security configuration framework to allow users to easily configure security options that can map to underlying complex Internet security protocols. Through this research, we aim to determine if these interventions can reinforce users' mental models, thereby improving Quality of Protection and Experience.

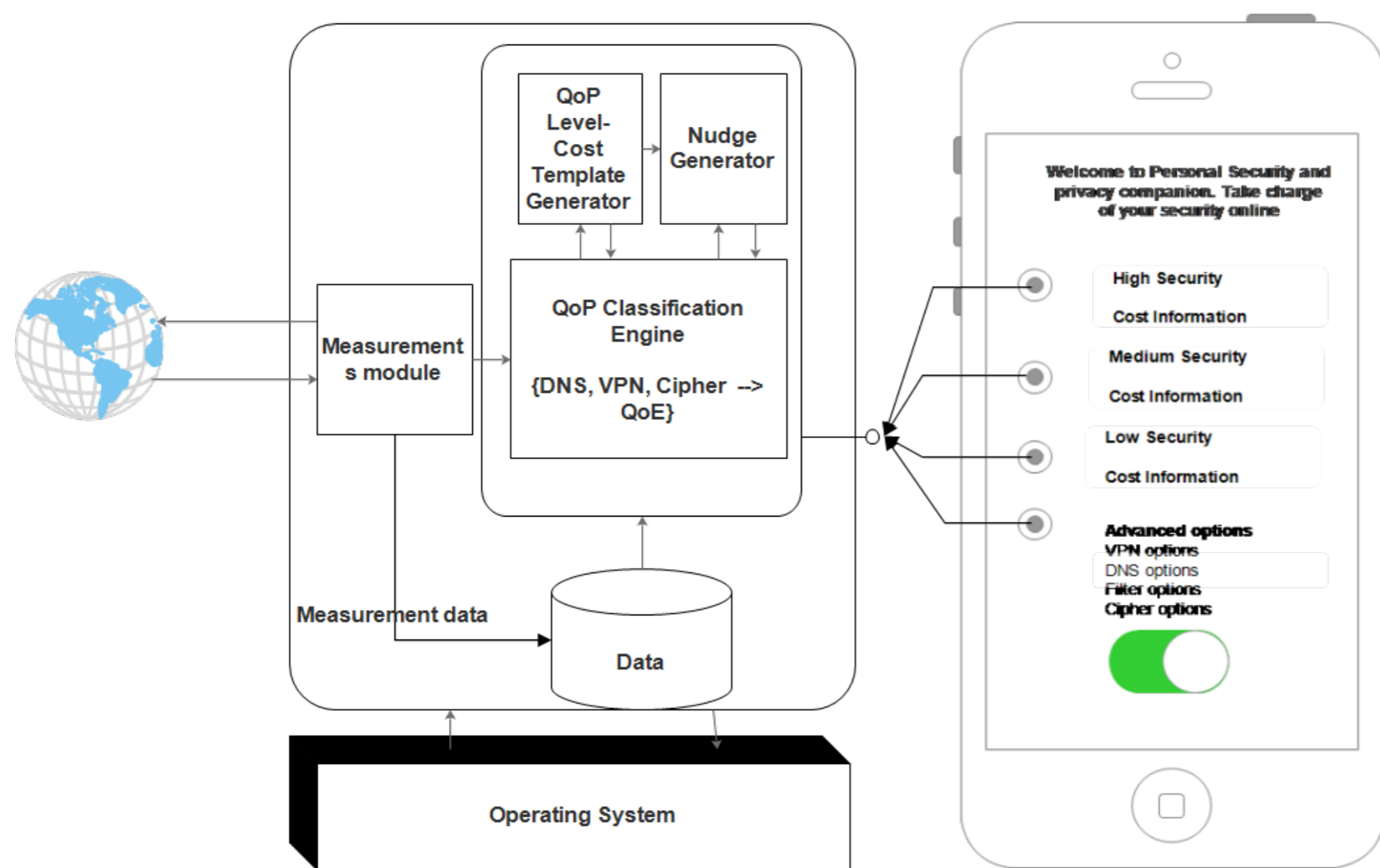
Motivation

- (a) Increased Internet userbase \Rightarrow Increased cybercrimes
- (b) So many complex security features not easily understood by average to novice Internet users. \Rightarrow Online Vulnerabilities
- (c) Internet security decisions centralised and hidden from users. \Rightarrow Disempowered to make optimal security decisions.

Research Questions

- (a) What is the relationship between users' computing skills level, security mental models, security preferences and Internet security practice?
- (b) What is the cost of Internet security protocols (i.e. secure DNS transactions, TLS, VPN) on the Quality of Internet browsing experience?
- (c) How would a personal security configurator impact users'
 - Quality of Protection and Experience?
 - mental models and security adoption?

Conceptual Framework



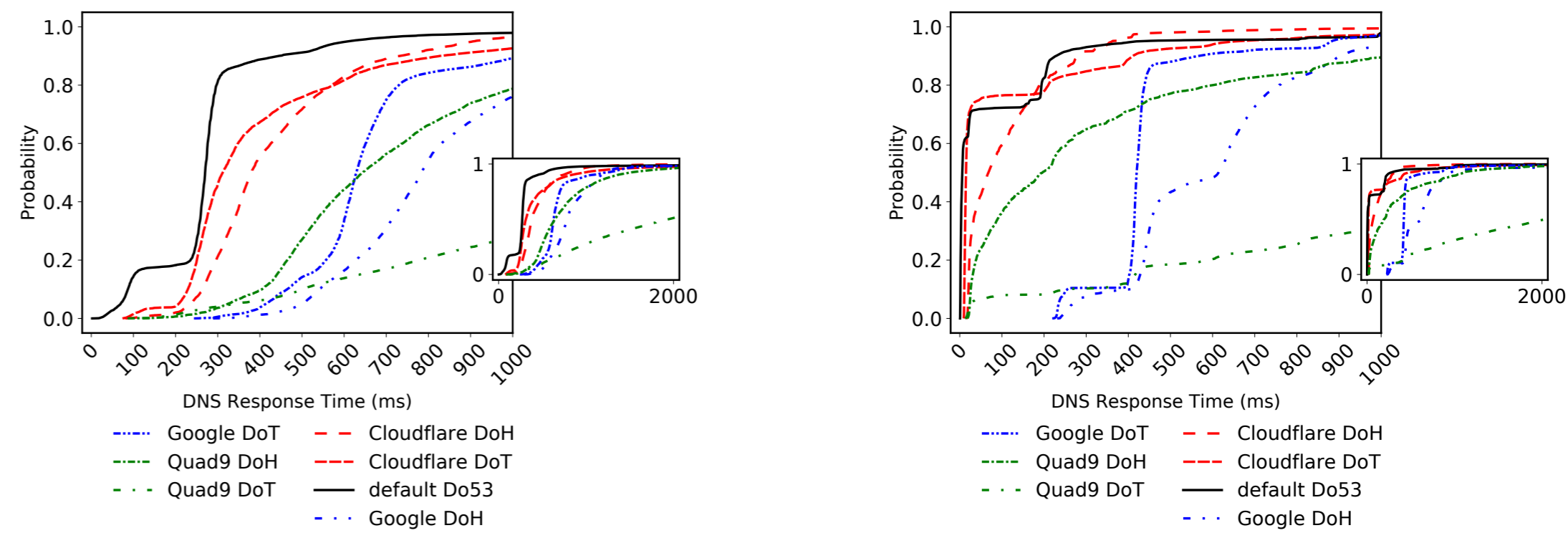
Research Contributions

- (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

Results- Question 1



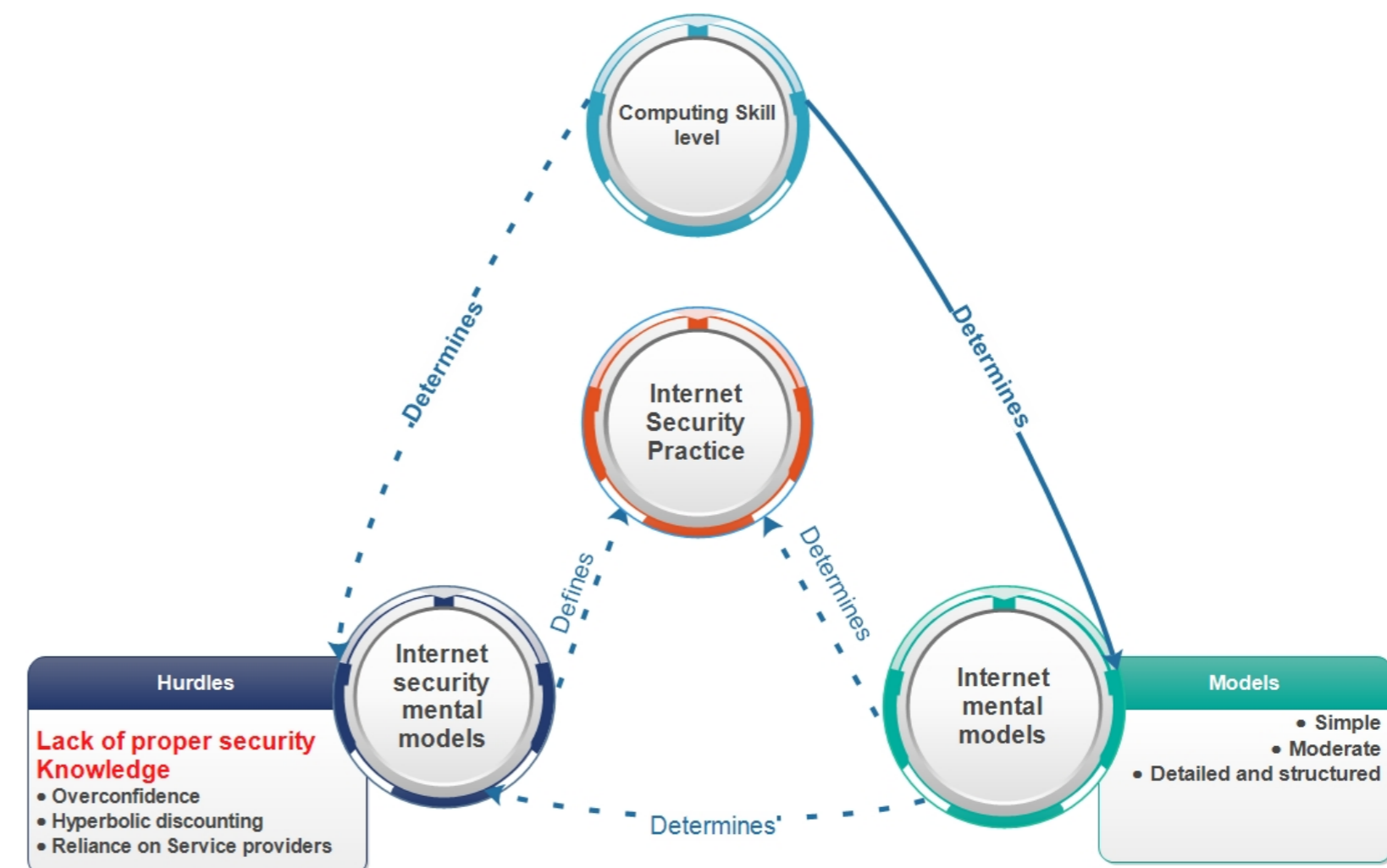
(a) DNS response time under 4G

(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

- Encrypted traffic always slower in low resource networks. Not always the case in higher resource networks
- User's choice of secure DNS provider and DNS protocols determines Quality of Experience
- DoE filtering improves QoE

Results - Question 2



- Better technical skills \Rightarrow better Internet models.
- Better technical skills \Rightarrow better online security practice
- Better security mental models \Rightarrow better security practice.
- Internet security configuration frameworks expert-oriented

Future Work

- (a) Evaluative Lab Experiments
- (b) Evaluative User Studies

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.