PowerQoPE: A Personal Quality of Internet Protection and Experience Configurator *

Enock Samuel Mbewe, Taveesh Sharma, and Josiah Chavula

University of Cape Town, School of IT, Department of Computer Science, Cape Town, South Africa
{embewe,tsharma,jchavula}@cs.uct.ac.za
http://www.uct.ac.za/

Abstract. Security configuration remains obscure for many Internet users, especially those with limited computing skills. This obscurity exposes such users to various Internet attacks. Recently, there has been an increase in cyberattacks targeted at individuals due to the remote workforce imposed by the COVID 19 pandemic. These attacks have exposed the inefficiencies of the non-human-centric implementation of Internet security mechanisms and protocols. Security research usually positions users as the weakest link in the security ecosystem, making system and protocol developers exclude the users in the development process. This stereotypical approach has negatively affected users' security uptake. Mostly, security systems are not comprehensible for an average user, negatively affecting performance and Quality of Experience. This causes the users to shun using security mechanisms. Building on human-centric cybersecurity research, we present a tool that aids in configuring Internet Quality of protection and Experience (referred to as PowerQoPE in this paper). We describe its architecture and design methodology and finally present evaluation results. Preliminary evaluation results show that user-centric and data-driven approaches in the design of Internet security systems improves users' Quality of Experience. The controlled experiment results show that users are not really stupid; they know what they want and that given proper security configuration platforms with proper framing of components and information, they can make optimal security decisions.

Keywords: Usable security · QoE · QoP · Internet Security · Cybersecurity.

1 Introduction

Internet usage has become part of our daily life, with its technologies affecting every part of our daily activities. The prevalence of smartphone usage has transformed the technology landscape, pushing the responsibility for one's digital data to the individuals. Security is one such responsibility that one must master to ensure cyber safety. Until the recent past, security has been considered corporates' responsibility and confined to a perimeter [1]. In this paradigm, most security systems are not designed for average users who form a greater part of the Internet user base. This kind of security implementation is referred to as *stupid user* or *paternalistic* security implementation [2, 3]. The exclusion of users in the security systems design robs them of the opportunity to acquaint themselves with necessary security knowledge, further deforming their security mental models and paralysing their online security practice [4]. The rapid penetration of mobile devices and personalised computing platforms has demolished security perimeters calling for a paradigm shift in security implementation. Security authors agree that security systems should be human-centric, considering three fundamental concepts: User, Usage, and Usability [1].

The latest advancements in technology, such as smartphone, the Internet of Things (IoT), and Wireless Sensor Networks (WSNs), however, has completely changed the landscape of cybersecurity. We now witness the increased cyber-attacks targeted at individuals abolishing any perimeters that existed. This means that individuals must be vigilant to protect their digital assets, making security configuration a personal responsibility. Some security researchers have proposed a paradigm shift from the human out-of-security loop to the human-in-the-security loop (human-centred cybersecurity or security orchestration). The argument is that if humans are involved in security decision making, they would have better security mental models, reinforcing their security practice. However, the Internet users' mental models have been reported to be flawed by the stupid user security implementation. Their proposal follows results from a series of usable and security usability research which found that certain user behaviours either positively or negatively impact their practice [5]. Such behaviours

* Supported by Hasso Platner Institute for Digital Engineering

usually are maintained throughout one's lifetime [6]. For example, overconfidence ("nothing bad can happen to me") and hyperbolic discounting (trading of security for short term benefits). These result in a privacy paradox, a situation where users' needs for privacy do not match their practice. The unfortunate part is that usually, users often underestimate the risks associated with such behaviours [7].

Internet security mechanisms and applications such as IP Security (IPsec), Virtual Private Networks (VPNs), Domain Name Systems (DNS), and Content filtering, among others, are some of the security systems that are yet to be designed for average users. DNS, for example, a fundamental component of the Internet, is barely understood by many users. Attackers exploit this weakness on one extreme who then successfully manipulate DNS records, monitor user transactions, and inject unsolicited ads and malware. Research shows that much as these can be configured by the user, they are usually hidden from the average user and are not fully comprehensible by this class of users. Demographics determine socio-technical approaches, which are very key in the Human-cyber space interaction. As such, security systems should target diverse classes of users. Usable security mainly focuses on systems and platforms. It seldomly touches on the usability of the underlying components of the Internet. Building on previous research, this paper focuses on the intersection of Quality of Security Services (also known as Quality of Protection (QoP)) and Quality of Experience (QoE). This paper collectively calls these services Quality of Protection and Experience (QoPE).

Previous work shows that most users do not configure Internet security, citing configuration complexity and overhead. Despite the failure to implement security, most Internet users acknowledge the need to stay safe online. Other reasons behind the non-implementation of security mechanisms include the negative effect of security on performance, especially in poorer network conditions. A user study by Mbewe and Chavula [4] showed that "flawed security practice does not only result from users' negligence, but also lack of sufficient Internet security knowledge." They, therefore, suggested that Internet security configuration frameworks should be designed with capabilities to reinforce users' security knowledge and mental models. This study focuses on DNS privacy, VPN, and content filtering. We follow a data-driven approach to ensure that the designed system reflects the network conditions under which the device is operating. We also incorporate nudging in the form of the high-level costs of the security settings. The contributions of this work lie in the quality of protection and experience. We argue that if the users are provided with different security configuration levels with their associated costs, they would be able to comprehend some of the security concepts that have been obscure to them and, in the long run, reinforce their security mental models leading to better security practice.

2 Background and Related Work

Security is generally defined as the collection of all measures to prevent loss of any kind. The security concept is as old as humankind, implying that human assets have been at risk ever since humanity existed. It can be categorised into two main groups: physical security and digital security. Physical security is mainly a personal responsibility, and, over time, humans have developed complex physical security mechanisms. This may be partly attributed to regular interaction and regular experimentation with the systems. Individuals can choose the level of security they need depending on the circumstances and on what they are protecting. Digital security, on the other hand, mostly follows a delegated approach modelled after power. Security researchers have for so long argued that security concepts are too complex to be understood by human beings. Hence, it is better to manage their security centrally where knowledgeable people can understand the concepts. Security was often seen as mathematical and technical. Following this line of argument, the same argument has been repeated by different researchers, with others coining humans as the weakest link in the security ecosystem. Thus, this kind of security implementation made sense in the era when the Internet was for the elite and corporates. In this paradigm, perimeter defence made sense.

2.1 Quality of Protection

The early research about human involvement in deciding the level of digital security was coined Quality of Security Service (QoSS) and later Quality of Protection (QoP) [8, 9, 10, 11, 12, 13]. This kind of research is aimed at balancing security and performance (throughput, latency and delay) or at least allowing the resource management systems to tradeoff security and performance. The idea came about because, generally, adding security to service increases the resource consumption and the delay of information exchange, thereby decreasing the Quality of Service(QoS), which, in turn, degrades

Quality of Experience (QoE) [14, 15, 16, 17, 18, 19]. Due to the multi-attribute nature of security, different researchers have focused on measuring the impact of specific security mechanisms on QoS and Quality of Experience (QoE). In an attempt to understand the impact of different encryption mechanisms on VoIP, studies [14, 15, 18] have shown that the IPSec protocol reduces jitter but significantly increases latency and end-to-end delay. They, however, recommend increasing bandwidth which might be expensive in low-resource networks. However, implementation of the proposed solutions followed the same paternalistic paradigm suiting the technological advancements of the time. The security applications developed using the recommendations from QoP research suffered a Single Point of Attack (SPoA), leading to a Single Point of Failure (SPoF). For example, Nahrstedt [8] proposed a middleware adaptation scheme to provide End-to-End tunable delay (QoS) and security. The scheme was later proven by Chen et al. [10] to be susceptible to Denial of Service bandwidth attack. To solve the identified weakness, Chen et al. [11] proposed a framework for integrating QoS and security and developing a security advisory system. Again, this solution was later proven to be susceptible to attack broadcasting. Despite the shortfalls, QoP research inspired the emerging human-centred security and Quality of Experience research.

For the majority of the users and applications, increased security cannot be achieved with technology that decreases usability. A study by Cardoso [20] proposes that the system interface be designed for ease of use so that users apply the protection mechanisms correctly. He argues that mistakes will be minimised if the users' mental image of their protection goals matches the security mechanisms. To design this mental model, Irvine [21, 22] developed a Quality of Security Service costing framework for quantifying costs related to security service. The study uses a security translation matrix developed by Ivirne [23], which maps the elements of a simple user interface i.e. *high, medium, low* to a detailed security invocation mechanism. The study quantifies the cost from *CPU time, memory, bandwidth, disk space, delay, jitter* and *latency.* The authors conclude by proposing that further research be conducted to determine formulae for calculating resource costs for a range of security services and determining the best units for cost measures. Much as their work focused more on resource management systems, they tried to untangle the misconceptions about security, users and QoS. Such works inspire our work in conjunction mental modelling research. We use the measurements approach to provide device-based security-performance costs.

3 System Design

3.1 Design Goals

The primary goal of our system is to assist Internet users, especially those with limited computing skills, to easily configure internet security settings on users' Internet access devices such as smartphones. These settings should be selected based on the network resources available on the device as well as the user's desired security level. For example, suppose the user experiences sub-optimal network performance at a given security level. In that case, they should be able to switch to a security level that provides better network performance. The system should also cater to the advanced category of users who have better understanding of their security configurations. These users usually desire autonomy in choosing the parameters that govern their smartphones' security and network performance. To achieve this, the system should allow a user to choose from all possible combinations of security parameters. Once a particular configuration is chosen and activated by the user, they should be able to also be able to test and monitor the performance of their connections. In addition, the system should be able to schedule tests periodically on the devices to collect performance data. The system should also be able to learn from this data and provide better informed security choices the next time a user requests for security configuration.

3.2 Choosing Parameters

Studies [24, 25] have shown that choice of DNS resolver preferences are pivotal to the level of QoE for users. Mbewe and Chavula [26] further measured the impact of applying DNS filters on QoE. Their results showed that apart from providing the user with an opportunity to choose an extra layer of protection, choice of filters impacts QoE. The authors also conducted a user study investigating Internet users' security mental models, their security configuration experience and general security practice [4]. Their results show inadequate Internet security mental models in self-reported expert and non-expert Internet users. Their mental modelling and task analysis revealed that the flawed security practice does not only result from users' negligence but also lack of sufficient Internet security knowledge. They finally recommended reinforcement of users' Internet security mental models through personalised security configuration frameworks to allow users, especially those with limited technical skills, to configure their desired security level easily. This work, therefore, builds on such works and presents a personal Internet security configuration companion. The following paragraphs outline the architecture, system components, and configuration parameters.

PowerQoPE integrates three privacy-centric protocols: DNS privacy (including DNS-based content filtering), VPNs and Transport Layer Security (TLS). These have been discussed in literature [4, 27, 28, 29, 30] and they offer a multiplicity of protections based on use case but mostly difficult to many novice Internet users. We use public DNS services as shown in Table 1, which have extensively been used in DNS privacy performance measurement works. All DNS providers except for Google have filter instances such as Security, Adult, Family and Ads filters. DNS filtering is a practice of blocking access to a domain for specific reasons such as content filtering. A site will be blocked if the contents it presents are deemed inappropriate by the configuration, such as gambling, malware, pornography, and unsolicited ads, among others. PowerQoPE uses known blocking databases and filter-enabled DNS services to help the user easily configure content filtering with minimal hustles. It further classifies commonly negotiated ciphers into strength levels using classes 3 to 5 as implemented in openSSL (level 5: high, level 4: medium and level 3 : low).

The user interface of our application is designed to provide four main levels of security - *high, medium, low, advanced.* Essentially, the user choice levels are determined by DNS protocol, VPN, web-filtering and cipher strength. For example, in the *high*, we use non-logging DoH (which is more private than DoT), remote VPN, and a stricter web filter. In the *medium* security option, we use DoT, local VPN, cipher strength level 4, and family filter. Finally, we use Do53, local VPN, cipher level 3 and Do53-based family filter in the low-security level. The outcome of a security decision by the server also depends upon the type of network to which the user's device is connected. For a given network type and configuration combination, the system returns the configuration with the least page load time. In the current implementation, only two network types are supported - *mobile (4G, 3G) and WiFi.* Once the user decides to use a particular configuration level, our system makes a security decision by allowing the configurations to be chosen from each of the below sets:

1. $\mathcal{D}$: A set of recursive DNS resolvers. Our current implementation supports the below recursive resolvers and their respective security filters as shown in Table 1. Each recursive resolver provides different options for the type of security filters. Each filter has three variants - DNS over port 53 (Do53), DNS over TLS (DoT), and DNS over HTTPS (DoH). In Table 1, for example, Cloudflare provides three distinct security filters, and each can be implemented with either Do53, DoT or DoH, giving 3 × 3 = 9 distinct options for the system to choose from.

DNS Provider	**Security Filters**
CloudFlare	No filter, Security, Family
Google	No filter
Quad9	No filter, Security
Cleanbrowsing	Family, Adult, Security
Adguard	No filter, Ad block, Family

Table 1: Different DNS providers and their security filter variants.

2. $\mathcal{C}$: A set of preferred cipher suites: As the name suggests, a cipher suite is a suite or a combination of ciphers responsible for authentication, key exchange, bulk encryption and signing.
3. $\mathcal{V}$: A set of publicly available VPN servers. Whenever the VPN mode is enabled in our system, the user's smartphone connects to a remote VPN server. These servers are chosen from a predefined list that contains servers that are freely available for academic use.

Formally, a security configuration can be denoted as a member of the set $\mathcal{D} \times \mathcal{C} \times \mathcal{V}$. Whenever the user chooses the advanced configuration, they have complete control over which member to choose from $\mathcal{D}$, $\mathcal{C}$ and $\mathcal{V}$. In all other cases, the system decides based on historical data, the user's current network type and the security level chosen. In our current implementation, VPN servers are only used when the user selects the high-security level or chooses to enable VPN at the advanced security level.

3.3 System Overview

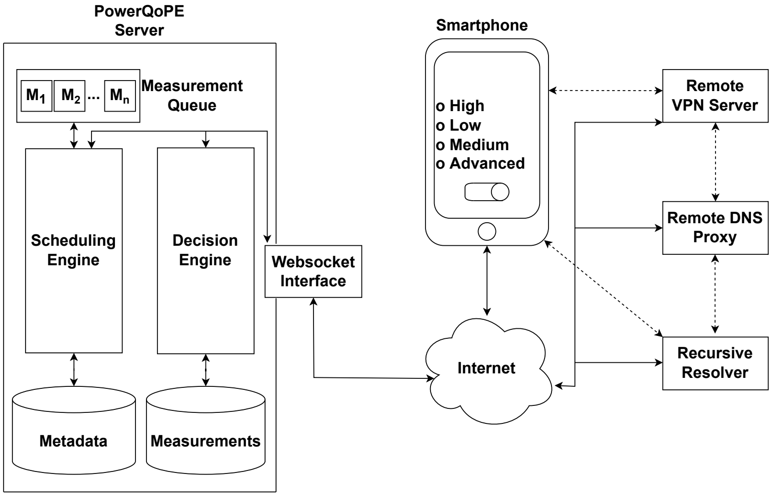


Fig. 1: An architecture of the proposed system, PowerQoPE. In this figure, the dotted arrows represent configuration-specific connections.

The PowerQoPE system (Fig. 1) is equipped to assist Android phone users in taking charge of their device's security. In the current implementation, the system can be used to collect measurement data and store it in the measurements repository for further analysis. All the security decisions made by the system are static and based on what has been observed previously by experimentation.

An orchestration engine forms the heart of the PowerQoPE system. A user can initiate three types of measurements from the Android application. These include speed tests, HTTP tests and video tests. Speed tests measure the latency, upload and download speed of data transfer between the nearest server and the user. HTTP tests provide insights about DNS response time, page load time and other related parameters when a website (either user-defined or system-defined) is visited from within the app. Video tests measure the buffer, load time and bandwidth for a system-defined video file. In the current implementation, these tests can only be initiated by the user.

For users who may be unfamiliar with terms like DNS, filters, VPN, cipher suites, the system provides three main security configurations - low, medium and high. As per previous experiments, if a stricter security level is chosen, the performance of applications that access the Internet is expected to degrade for poorer connections. Thus, users with a very high-quality internet connection can enjoy the benefits of maximum security that could be configured.

The Android application provides an advanced options radio button for a technically capable user. On tapping this button, they can choose the specific DNS provider and the type of filter (family, advertisements, security) depending on whether it is available with the provider or not. Since the list of supported cipher suites is large, the application only provides the category of the cipher (low, medium, high) as an option. If a user selects a specific cipher category, all ciphers belonging to that category are sent to any subsequent HTTP request made from within the app.

3.4 Architectural Components

PowerQoPE server This component is responsible for orchestrating the measurements, including HTTP webpage downloads, speed tests and video tests. The design of this measurement server is a modified version of QoSMon, an architecture proposed by Sharma and Chavula [31]. One key modification to this design allows measurements to be scheduled on a specific device instead of any device.

- **Measurements Scheduling Engine:** This component allows measurements to be scheduled periodically on end-user devices by minimising the contention between network and CPU resources used by measurements. This engine can be configured to use four existing measurement scheduling algorithms [32].

- **Decision Engine:** There are two main categories of decisions that the PowerQoPE server is involved in. The first decision is related to selecting the best DNS configuration for a user. The decision engine searches the historical data and finds out all the configurations with the same network type and chosen level of security. Then, it chooses a single configuration that corresponds to the least page load time. The second decision is related to choosing a VPN server when the user has selected a high configuration. The PowerQoPE server maintains a list of freely available VPN servers and updates it every 30 minutes with their latest configurations. Then, when asked to decide, the server chooses a single VPN server with the lowest latency and the highest throughput.
- **Remote DNS proxy:** This proxy is used in configurations where remote VPN capabilities are enabled. Our application uses OpenVPN [33] for configuring a new VPN server, and it requires the recursive resolver's IP address to be written in a configuration file. This works well for Do53 and DoT, but not in the case of DoH because it requires the complete URL of the recursive resolver instead of the IP address. Therefore, we decided to relay all DoH requests through a proxy that we configured beforehand with a particular DoH-based resolver.

User application module The user application module (See Figure 2) handles user configurations and user-initiated measurements. It comprises a user interface, measurements module, nudge generator and the QoPE configuration module. The user module handles user preferences and configures them on the operating system. In the current implementation of PowerQoPE, only Android phones are supported. The Android user application is designed so that it persists its connection with the server even when the user switches from one network to another. We now briefly describe each of the user module components:

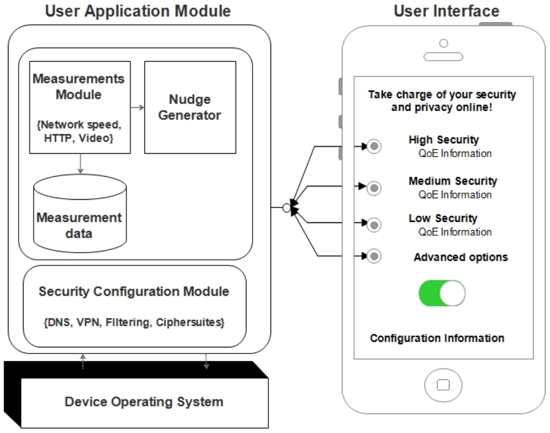


Fig. 2: User application module components and user interface wireframe

- **QoPE configuration Module**: The QoPE configuration module handles user preferences based on the decisions and classifications made by the PowerQoPE server and configures them on the device. The user can as well overwrite server recommendations by performing the advanced configuration. Currently, the module can configure DNS (Do53. DoT and DoH), web filtering, VPN and cipher suites. We provide the user with high-level choices; low, medium, high and advanced. The app connects to a local VPN server in low and medium configurations. It resolves any subsequent HTTP requests via a recursive resolver recommended by the server. In high configuration or any other configuration with VPN enabled, the app connects to a remote VPN server. This remote server can either be chosen by the user or recommended by the system, depending on whether the advanced configuration is selected. All subsequent HTTP requests are sent through the VPN tunnel and resolved via a remote DNS proxy in this type of setting.

4 Evaluation

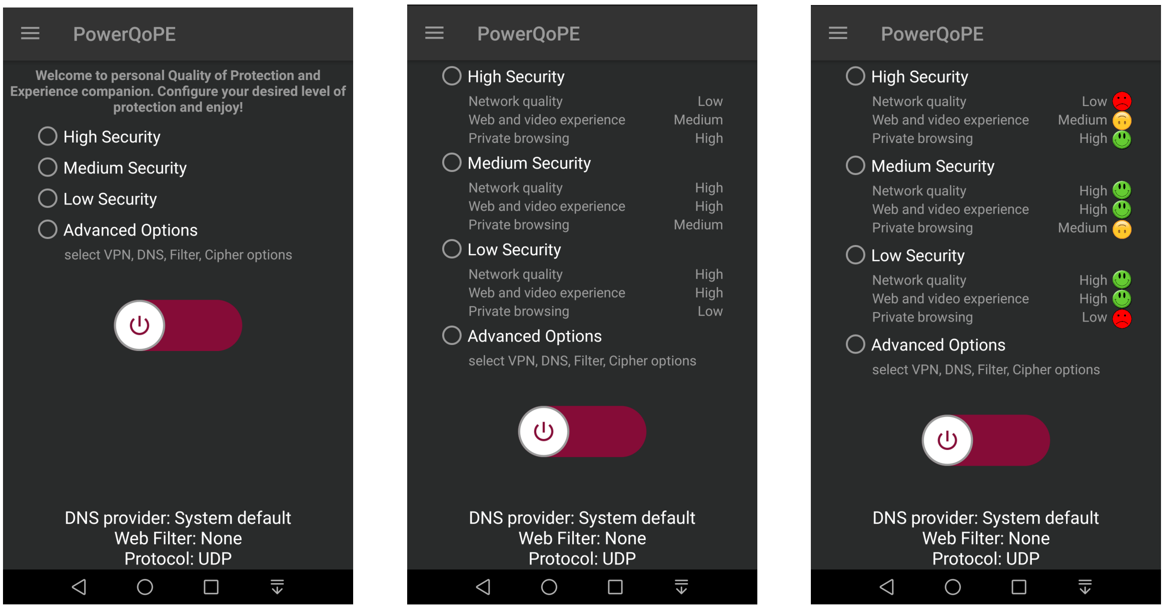
4.1 Methodology

This section describes the procedure followed to evaluate the components of PowerQoPE. We conducted an evaluative controlled user experiment to test the effectiveness of personal Internet security configuration tool, especially on the configuration options and security-performance cost. The experiment aimed to assess whether providing Internet users with levels of security configuration and accompanying the levels with their associated performance or privacy cost would modify user's security choice.

Participants To ably evaluate the usefulness and inform further design of the app, an initial usability study was carried out with 14 participants (seven females and seven males). These users were novice frequent Internet users with a basic understanding of computing. Purposive sampling of participants was used to get ideas from a specific cadre of Internet users, i.e. novice Internet users. All the participants completed high school and understood English.

Design Three interfaces (See Figure 4.1) of security configurations were designed to assess whether adding the performance cost of different security configurations would help users make an informed security decision. The first interface had only the security configuration levels (High, Medium, Low and Advanced). The second screen was activated by toggling a button. On toggling, descriptive costs of the underlying security mechanisms were added under each security option, categorised under network quality, video streaming quality and security/privacy. We decided to use a within-subject controlled user experiment [34] approach to fully measure if the protection motivation features of the app would modify users' security and QoE mental models. Within-subjects experimental design demands that each participant tests all the conditions under study. In our case, each participant performed all the three tasks.

In order to test whether security costs and visual cost framing, in addition to the security levels, would improve the security mental models and encourage users to configure better security, we provided different interfaces of the personal security configuration tool, enabled by toggling different combinations of the configurations. First, we have security levels with no cost information (LCn) as control (See Figure 3a). Then, security levels with textual cost Information (LC, Figure 3b) and security cost with visual cost framing (LCV, Figure 3c). We further randomised the order of the security options for each task.



PowerQoPE

Welcome to personal Quality of Protection and Experience companion. Configure your desired level of protection and enjoy!

○ High Security
○ Medium Security
○ Low Security
○ Advanced Options
select VPN, DNS, Filter, Cipher options

DNS provider: System default
Web Filter: None
Protocol: UDP

(a) First screen containing security configuration levels only

PowerQoPE

○ High Security
Network quality Low
Web and video experience Medium
Private browsing High
○ Medium Security
Network quality High
Web and video experience High
Private browsing Medium
○ Low Security
Network quality High
Web and video experience High
Private browsing Low
○ Advanced Options
select VPN, DNS, Filter, Cipher options

DNS provider: System default
Web Filter: None
Protocol: UDP

(b) Second screen containing security configuration levels with their associated textual cost information

PowerQoPE

○ High Security
Network quality Low ☹
Web and video experience Medium 😐
Private browsing High ☺
○ Medium Security
Network quality High ☺
Web and video experience High ☺
Private browsing Medium 😐
○ Low Security
Network quality High ☺
Web and video experience High ☺
Private browsing Low ☹
○ Advanced Options
select VPN, DNS, Filter, Cipher options

DNS provider: System default
Web Filter: None
Protocol: UDP

(c) Third screen containing security configuration levels with their associated textual and graphical cost information

Fig. 3: Configuration screens for tasks 1 to 3

Materials The experiment required the following materials:

- A smartphone with android operating system.
- A mobile application which we developed iteratively for this purpose.
- Deliberate configuration of three different interfaces that visibly showed different elements.
- An interview guide used as a follow up between tasks.

Procedure The Ethical clearance was sought from our University's ethics committee. The experiment was conducted at a telecentre on Likoma Island in Malawi. The location was ideal because there was an ongoing project to sensitise the youth on general cybersecurity. The researcher had no relationship with the participants, and the experiment was not related to the project.

The convener welcomed the participants, and explained the aim of the experiment. Then the participants were given an online informed consent form to read and, if in agreement, sign. It was emphasised that participants were free to withdraw from the study. Then the participants completed a pre-experiment questionnaire that captured demographics and assessed their Internet security knowledge. No identifying information was collected. Finally, the participants were assigned unique IDs.

The participants were asked to install the app on their smartphones. The experiment began when participants indicated that they were ready. Participants were asked to open the PowerQoPE app they had just installed. Then they were asked to choose their desired protection level from a list of radio buttons (High, medium, low, advanced). Then the participants were asked to run the measurements module (both Internet speed and web QoE) using their security choice. This was specifically done to collect empirical performance cost of the selected security level. The participants were asked to give a rationale for their choice marking the end of the first task. The researcher recorded the responses on a notepad. There was a lapse of 15 minutes between the tasks.

Then the researcher toggled the cost information for each security option. The order of the security options was shuffled (i.e. medium, low, high) to minimise learning effects. The participants were asked to choose their desired level of protection, this time, based on the cost information visible. Again, they were required to run the measurements module if their choice in Task 1 differed from their choice in Task 2. The researcher asked them to explain their choice, and the responses were recorded.

Finally, the researcher toggled visual cost. This setting only appended simile faces to the cost information. The participants were asked to repeat the tasks. Participants' preferences were recorded for each task and summarised.

5 Results

This section provides two sets of results; analysis of the user experiment and results from the measurements.

5.1 Influence of security cost information on users' choice of security level

Users' security options for each task were tabulated and compared. Figure 4 shows participants' security preferences against conditions. Recall that Task 1 only provided the security levels from which the participant was required to choose one option based on the PMT's framing of the options and their mental models. Task 2 added textual cost information to the security levels. The cost information was qualitative to avoid suffocating the participant with technical details. The costs were based on network performance, browsing/streaming experience and security/privacy.

The results show that 100% of participants chose the high-security option in Task 1. When textual information was added in Task2, 50% of the participants changed their preference to medium while 21% chose low security. Finally, when visual cost nudges were added to the cost information, 71% of the participants chose medium security, 21% chose high security, and only 1 (8%) chose low security.

When asked why they configured high security in Task 1, many responded that they "care about security and secure connection". However, when presented with cost information, the same 71% of the participants changed from a high-security configuration. When asked about the sudden change of preference, one participant said,

> *"Slow internet flustrates, I would rather have a combination of good Internet performance and security, hence my change from high to medium-security..*"

Three (3) participants switched from high security to low security. When asked why they chose low security, the participants said they would rather compromise security but not Internet speed.

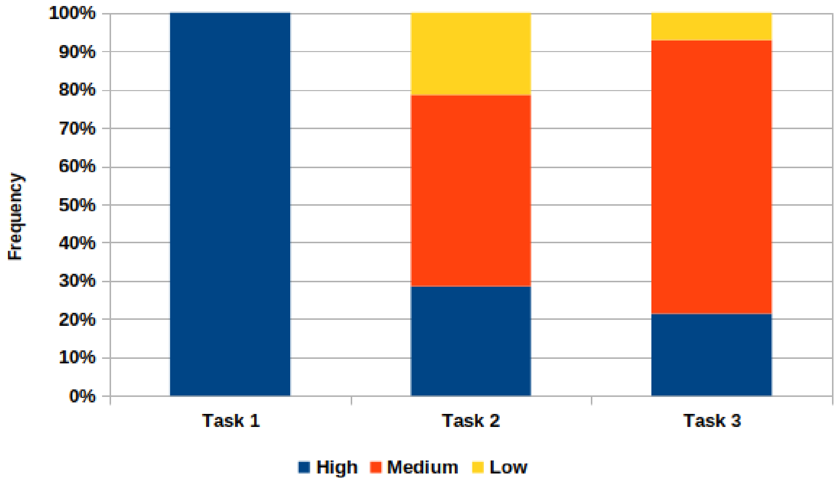
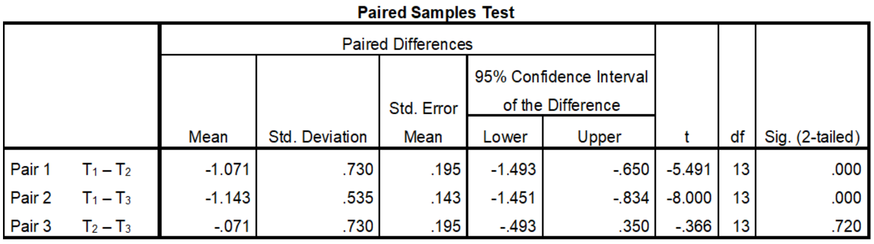


Fig. 4: Participants' security preferences for each condition (Task 1: Security levels only, Task 2: Security levels plus textual performance cost, Task 3: Security levels, textual and visual performance cost)

Task 3 results did not differ much from Task 2's. However, two of the three who chose the low-security option in Task 2 changed to medium-security. When asked why that change, one participant attributed the change to the images that accompanied the cost information saying that the visual nudges made the costs more visible.

We finally run paired t-tests between tasks to determine whether the differences were significant. We first compared Task 1 and Task 2, then Task 1 and Task 3 and finally Task 2 and Task 3. In short, we present the combinations as $T_1 - T_2$, $T_1 - T_3$ and $T_2 - T_3$, where T stands for "Task" as shown in Figure 5.



Paired Samples Test

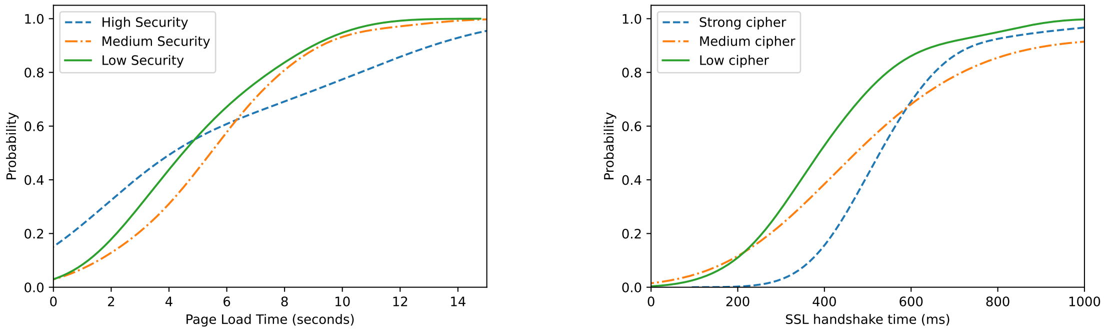
		Paired Differences					t	df	Sig. (2-tailed)
					95% Confidence Interval of the Difference				
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper			
Pair 1	$T_1 - T_2$	-1.071	.730	.195	-1.493	-.650	-5.491	13	.000
Pair 2	$T_1 - T_3$	-1.143	.535	.143	-1.451	-.834	-8.000	13	.000
Pair 3	$T_2 - T_3$	-.071	.730	.195	-.493	.350	-.366	13	.720

Fig. 5: Paired samples test

From Figure 5, we observe a significant difference between Task 1 and Task 2 ($p = .000$), Task 1 and Task 3 ($p = .000$). We observe no significant difference between Task 2 and task 3 ($p = .720$). This tells us that cost information, whether textual or combined with graphical costs, can modify users' security preferences. The results also show that adding a visual nudge to the textual cost information does not significantly affect users' security preferences.

5.2 Empirical performance impact of Users' choice of security level

Descriptive statistics were used to analyse the measurements data. Figure **??** show empirical performance impact impact of users' security choice. Metrics of interest were page load time, DNS response time, network speed and SSL time. Due to space limitation, we will consider pageload time and SSl time.



(a) Page load time for each of the security configuration levels

(b) SSL handshake time for each of the security configuration levels

Fig. 6: User initiated measurement results

Figure 6a shows page load time CDF for security levels. Generally, we see that high security is slower than the medium and low-security options. However, we see that high-security options outperform both medium and low levels for faster loading pages. We suspect that such faster loading websites are at the top of the tranco list and have caches within Africa. In general, we observe that high-security configuration results in longer page load time while medium level has moderate PLTs followed by low-security level. Similar patterns are observed in Figure 6b which shows the impact of cipher suite strength on SSL time which in turn affects page load time. However, higher strength ciphers outperform medium strength ciphers for the not-so-famous websites, i.e. websites at the tail of the tranco list. [1]. This is because most preferred stronger ciphers perform 1 round trip while medium ciphers perform 2 round trips. Therefore, higher latency domains will incur longer SSL handshake time.

6 Discusion

Thus far, we have presented the design and preliminary evaluation of a security configuration tool called PowerQoPE. Using the concepts of the Protection Motivation Theory (PMT), we included some features that would nudge the user into implementing a desired level of security. We then conducted a controlled user experiment to evaluate the feasibility of such features, i.e. QoE impact of different security mechanisms.

From the results, we observe that the participants implemented a high-security option in the absence of cost information. However, when cost information was added, most participants changed their preference. In this case, the users weighed the negative effects of relaxing security in trying to enjoy good Internet speed. The change was also possible because options were within reach of participants. The participants were novice Internet users. The complex underlying security constructs were hidden under advanced security options. This simplified and minimised novice participants' search space. Using this prototype, novices could configure VPN, DNS and content filtering, defeating the stereotype that security is so complex for an ordinary user.

We further note that other users would still choose suboptimal security configuration even in the presence of the options. This fact cannot be ignored for Internet users with a persistent slow connection. To this type of users, it makes sense to restrict the options to ensure that there always exists a minimum possible security level; otherwise, such users may give up security for speed. This cognitive bias is known as hyperbolic discounting [2]. In this situation, one chooses short time benefits disregarding the long time consequences.

Empirically, we found that the cost displayed to the user closely represented the actual impact of the underlying security mechanisms. We also note that the choice architectures implemented in the prototype maps the objective measurement results. This suggests that data-driven security decisions would improve the QoE even if the user configures a high-level security option. We see from the empirical measurements results that participants used slower networks as evidences by longer page

[1] See https://tranco-list.eu/latest_list

load times. These are typical speeds offered by mobile service providers in most parts of Africa. Therefore, adaptive security configuration solutions such as PowerQoPE would assist users under such network conditions to decide the level of security based on their network conditions.

We argue that properly designed security configuration tools would bridge the divide between novice and expert users while still aiding in optimal security decision-making. This calls for more studies and experiments on user-centric security. This may lead to different use cases integrated into the security configuration interfaces of devices from different vendors and operating systems such as smartphones, SOHO routers and others.

The apparent limitation of this study lies in the sample size and diversity of participants. The sample size of 14 participants may not give us generalisable results. Also, we tested this on novice users from one geographical location. However, we argue that the results provide insights into how Internet security configuration protocols can be designed to involve novice users in the security decision making. Such platforms can be used to reinforce users' security mental models thereby improving their online security practice.

7 Conclusion and Future work

In this paper, we have shown that complex security configurations can be made available to novice users who have generally been regarded as the weakest link in the security ecosystem. Future work will expand the evaluation with more participants of diverse demographics. Future works also include testing Usefulness, Satisfaction and Ease of use.

Acknowledgments

The authors are grateful for the financial support received from the Hasso Plattner Institute for Digital Engineering through the HPI Research School at the University of Cape Town. In addition, the authors would like to thank *Mr Henry Mikanda* for helping with UI design and *Mr Joseph Kumwenda* for the help rendered during data collection. Finally, we thank all the participants for their time and willingness to provide information published in this study

References

[1] M. Grobler, R. Gaire, and S. Nepal, “User, Usage and Usability: Redefining Human Centric Cyber Security,” *Frontiers in Big Data*, vol. 4, mar 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7968726/

[2] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. L. F. Cranor, S. Komanduri, P. G. P. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson, “Nudges for privacy and security: Understanding and assisting users’ choices online,” *ACM Computing Surveys*, vol. 50, no. 3, aug 2017.

[3] R. Wash and E. Rader, “Influencing mental models of security: A research agenda,” *Proceedings New Security Paradigms Workshop*, 09 2011.

[4] E. S. Mbewe and J. Chavula, “Security Mental Models and Personal Security Practices of Internet Users in Africa,” in *e-Infrastructure and e-Services for Developing Countries*, Y. H. Sheikh, I. A. Rai, and A. D. Bakar, Eds. Cham: Springer International Publishing, 2022, pp. 47–68.

[5] N. Gcaza, R. von Solms, M. M. Grobler, and J. J. van Vuuren, “A general morphological analysis: delineating a cyber-security culture,” *Information & Computer Security*, 2017.

[6] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, “Risk perceptions of cyber-security and precautionary behaviour,” *Computers in Human Behavior*, vol. 75, pp. 547–559, 2017.

[7] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey, “Users really do plug in USB drives they find,” in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 306–319.

[8] K. Nahrstedt, “An integrated solution to Delay and Security support in wireless networks,” in *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, vol. 4, April 2006, pp. 2211–2215.

[9] J. Chen, C. Hu, H. Zeng, and J. Zhang, “Impact of Security on QoS in Communication Network,” in *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, April 2009, pp. 40–43.

[10] T. Taleb, Y. Hadjadj Aoul, and A. Benslimane, “Integrating Security with QoS in Next Generation Networks,” in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, Dec 2010, pp. 1–5.

[11] T. Taleb and Y. Hadjadj-Aoul, “QoS^2: a framework for integrating Quality of Security with quality of service,” *Security and Communication Networks*, vol. 5, no. 12, pp. 1462–1470, 2012. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.523

[12] B. Ksiezopolski, T. Zurek, and M. Mokkas, “Quality of Protection Evaluation of Security Mechanisms,” in *The Scientific World Journal*, 2014.

[13] D. Rusinek, B. Ksiezopolski, and A. Wierzbicki, “AQoPA: Automated quality of Protection Analysis Framework for Complex Systems,” 09 2015.

[14] P. Radmand and A. Talevski, “Impact of Encryption on QoS in VoIP,” in *2010 IEEE Second International Conference on Social Computing*, Aug 2010, pp. 721–726.

[15] H. A. Mohammed and A. H. Ali, “Effect of some Security Mechanisms on the QoS VoIP application using OPNET,” *International Journal of Current Engineering and Technology*, vol. 3, pp. 1626–1630, 12 2013.

[16] A. Hani Haidar, M. Houseini, and M. Kshour, “The Analyse of Adding security on QoS parameters,” *International journal of innovative research in advanced engeneering*, vol. 2, 11 2015.

[17] S. Lindskog and E. N. Jonsson, “Adding Security to Quality of Service Architectures,” 2002.

[18] A. A. Al-khatib and R. Hassan, “Impact of IPSec Protocol on the Performance of Network Real-Time Applications: A Review,” *I. J. Network Security*, vol. 20, pp. 811–819, 2018.

[19] T. Hayajneh, B. Mohd, and A. Itradat, “Performance and Information Security Evaluation with Firewalls,” *International Journal of Security and Its Applications*, vol. 7, pp. 335–372, 11 2013.

[20] L. S. Cardoso, “Quality and Security Usability,” in *ITU-T Wksp. End-to-End QoE/QoS*, Geneva, Switzerland, June 2006, pp. 721–726.

[21] C. Irvine and T. Levin, “Toward a taxonomy and costing method for security services,” in *Proceedings 15th Annual Computer Security Applications Conference (ACSAC’99)*, Dec 1999, pp. 183–188.

[22] E. Spyropoulou, T. Levin, and C. Irvine, "Calculating costs for Quality of Security Service," in *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)*, Dec 2000, pp. 334–343.

[23] E. Irvine, Cynthia, "A note on mapping user-oriented Security policies to complex mechanisms and services," 1999. [Online]. Available: https://calhoun.nps.edu/handle/10945/15290

[24] Mbewe, Enock S.and Chavula, Josiah, "On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters," in *Towards new e-Infrastructure and e-Services for Developing Countries*, Zitouni, Rafik and Phokeer, Amreesh and Chavula, Josiah and Elmokashfi, Ahmed and Gueye, Assane and Benamar, Nabil, Ed. Cham: Springer International Publishing, 2021, pp. 289–304.

[25] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, "Analyzing the costs (and benefits) of DNS, DoT, and DoH for the modern Web," july 2019. [Online]. Available: https://arxiv.org/pdf/1907.08089.pdf

[26] E. S. Mbewe and J. Chavula, "Measuring QoE Impact of DoE-based Filtering," in *Proceedings of Southern Africa Telecommunication Networks and Applications Conference.* Champagne Sports Resort, Central Drakensberg, KwaZulu-Natal, South Africa,: SATNAC, 2021, pp. 240–245. [Online]. Available: https://pubs.cs.uct.ac.za/id/eprint/1508/

[27] I. Ion, R. Reeder, and S. Consolvo, ""...No one can hack my mind": Comparing expert and non-expert security practices," *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*, pp. 327–346, 2019.

[28] M. G. Maceli, "Encouraging patron adoption of privacy-protection technologies:: Challenges for public libraries," *IFLA Journal*, vol. 44, no. 3, pp. 195–202, 2018.

[29] R. W. Reeder, I. Ion, and S. Consolvo, "152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users," *IEEE Security and Privacy*, vol. 15, no. 5, pp. 55–64, 2017.

[30] Y. Zou, K. Roundy, A. Tamersoy, S. Shintre, J. Roturier, and F. Schaub, "Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices," *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1–15, 2020.

[31] T. Sharma and J. Chavula, *Investigating Measurement Scheduling Strategies in Low Resource Networks (Poster).* New York, NY, USA: Association for Computing Machinery, 2021, p. 453–456. [Online]. Available: https://doi.org/10.1145/3460112.3472310

[32] Sharma, Taveesh and Chavula, Josiah, "Topology-Aware Measurement Scheduling Strategies in Low Resource Networks," in *Proceedings of Southern Africa Telecommunication Networks and Applications Conference (SATNAC), Central Drakensberg, South Africa.* SATNAC, 2021, pp. 308–313.

[33] M. Feilner, *OpenVPN: Building and integrating virtual private networks.* Packt Publishing Ltd, 2006.

[34] A. J. Anderson, "Controlled experiments," *Interpreting Data*, pp. 183–190, 2019.