Measuring QoE Impact of DoE-based Filtering

Enock Samuel Mbewe, Josiah Chavula
Department of Computer Science , University of Cape Town, South Africa
{embewe,jchavula}@cs.uct.ac.za

***Abstract*—In this paper, we analyse the impact of DNS-based filtering on Quality of Experience (QoE). We use three DNS standard protocols: regular DNS (Do53), DNS over HTTPS (DoH) and DNS over TLS (DoT) on Quality of Experience. We conduct measurements against four open public DNS service providers (Cloudflare, CleanBrowsing, Adguard and Quad9) under three network conditions; Campus wired network, Eduroam and 4G. We aim to establish whether the filters from the same provider have statistically significant differences. This information could be used by Internet users and Internet Service Providers to make sound decisions when choosing DNS privacy services. The results show significant DNS response time and page load time differences between non-filtered and filtered DNS recursive resolvers from Cloudflare, Adguard and Quad9. We do not observe significant differences in page load times when CleanBrowsing resolvers are used despite observing significant differences in DNS response times. The results further show that some filters would provide better QoE than non-filtered counterparts.**

***Index Terms*—Internet performance, DNS privacy, DNS measurements, DNS filtering, QoE, QoP, DoH, DoT, Do53**

I. Introduction

Domain Name System (DNS)[1] is a fundamental component of the Internet that maps the human-readable names to their respective IP addresses of Internet resources. For most of the Internet's history, these services have been delivered in plaintext, providing a fertile ground for attackers to exploit and compromise Internet users' security and online privacy [2]. As a result, various efforts have been developed to encrypt DNS queries. These efforts have resulted in the development of different protocols such as DNS over TLS (DoT) [3], DNS over DTLS, DNS over QUIC, DNS over HTTPS (DoH)[4], DNSCrypt [5] and DNSCurve [6]. DNS over HTTPS (DoH) and DNS over TLS (DoT) are the two newer standard protocols requiring more studies to understand them fully. Both these protocols encrypt DNS traffic to improve the privacy of Internet users. Our study focuses on these two protocols as measured from end-user networks and devices. We collectively refer to these protocols as DNS-over-Encryption (DoE), a term that was introduced by Lu *et al.* [7]. We use DNS over port 53 (Do53) to refer to the regular, unencrypted DNS.

Given the recency of DoT and DoH, the Internet measurements research community is yet to establish the real performance cost of these protocols. At the writing of this paper, we know of very few measurement studies on the performance cost of DoT and DoH. An early preliminary study by Mozilla [1] found that DoH lookups are only marginally slower (6 ms) than conventional, unencrypted DNS over port 53 (Do53). Bottger *et al.* [8] studied the DoH ecosystem to understand the cost of the additional DNS security. Their findings indicate that the impact is marginal and does not heavily impact the page load times. In their works, Hounsel et al. ([9] and [10]) compared the cost of DoT and DoH measured from campus network and Amazon ec2 instances. Their results show that despite the lower resolution times of Do53, DoT and DoH can perform better than Do53 in terms of page load times. Lu *et al.* [7] conducted end-to-end DNS-over-Encryption measurements. They report that generally, the service quality of DNS-over-Encryption is satisfying in terms of accessibility and latency. In our prior work[2], we found that DoT and DoH negatively impact QoE, especially when the content is hosted offshore using offshore resolvers. We concluded the study by calling for ISPs and network operators to implement DoE and hosting services closer to their subscribers. In the current paper, however, we investigate whether using filters would improve QoE.

DoH, in particular, is attracting the attention of the research community due to its current centralised implementation. As a response, some works focus on de-centralising DoH so that no single provider has all the browsing information. Hoang *et al.* [11] propose K-resolver to slice user information to different decentralised DoH resolvers. This decentralisation, however, suffers from increased latency when the servers are geographically separated. A similar study is conducted by Hounsel *et al.*[12] which proposes a distributed DoH server architecture called M-DNS. However, none of the works so far has evaluated the cost and potential benefits of DoE-based filtering on Quality of Experience.

DNS-based filtering is one of the add-on services that Internet Service Providers (ISPs) have been offering to their subscribers to protect them from malware [13], adware, botnets [14], [15] phishing, cyberbullying and pornography. However, RFC 7258 [16] classifies such filtering mechanisms as pervasive monitoring. This leaves the ISPs in a dilemma since these mechanisms also protect their infrastructure apart from protecting their clients. This has led to resistance by ISPs from adopting DoH, which sends DNS transactions over HTTP traffic [17]. The Internet research community has tried and continues to measure the impact of DoE protocols on QoE. Analysing the ensuing performance impact of such protocols and their filtering services would be critical to both ISPs and the end-users.

This paper presents the results of DNS security measurement study taken from 13 vantage points located in 7 African countries (including the name of the Internet provider): Mada-

[1]See https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results

gascar (Widecom), Zambia (MTN, Liquid telecoms), Uganda (Airtel, Orange), Kenya (Airtel), Nigeria (MTN), Malawi (TNM, Airtel) and South Africa (Vodacom, Eduroam, Campus wired network). We conduct the measurements on end-user devices against 11 resolvers from Four DNS providers; Adguard [AdGuard Nofilter (AGN), Adblock/Security filter (AGAd/AGS), AdGuard Family filter (AGF)], CleanBrowsing [CleanBrowsing Adult filter (CBA), CleanBrowsing Security filter (CBS), CleanBrowsing Family filter (CBF)], Cloudflare [Cloudflare Nofilter (CFN), Cloudflare Security filter (CFS), Cloudflare Family filter (CFF)], and Quad9 [9 Nofilter (Q9N), Quad9 Security Filter (Q9S)]. We compared the performance of these resolvers to the local, Do53 resolver provided by the network.

We perform these measurements on 4G, Eduroam and Wired networks. We compare the DNS response time and page load time when different filters are configured. We measure the performance of both filtered and non-filtered configurations on each recursive resolver on the three protocols; regular DNS (Do53), DoT and DoH. We further measure the performance of the local recursive resolver's non-filtered Do53 to serve as a baseline. The main objective of this study is to establish whether DNS filters from the same provider are significantly different. We further investigate the implication of DNS response times and page load times.

Contributions: The contributions of this study are as follows:

- *Performance analysis of DoE-based filtering (from the vantage point of access networks in Africa.)* We conduct baseline internet measurements from real access networks in Africa. The results from these measurements can inform the Internet community on the best DNS filter provider to use depending on their geolocation and network conditions. This contribution is two-fold: First, the ISPs can learn from the performance of these open public resolvers and implement their own local, filter-enabled DoE infrastructure, which would reduce latency to the DoE servers. This would lead to lower DNS response times and page load times. Secondly, the results from this study inform the user which filters would result in better QoE.
- *Observations.* Using the dataset collected, we compare the performance impact of DNS-based filtering using public DoE resolvers. For example, we observe higher DNS response times from Adguard's filters. This information may help the DNS providers to optimise their services for networks in Africa.

II. Methodology

The study uses Alexa's top 50 global websites for African countries and the top 50 local ones for each African country (hosted locally or operated by local entities). The local websites were particularly included to represent the websites serving African content and observe how DoT and DoH impact the browsing QoE on the local websites. We managed to get 1583 unique websites that we use in this study.

A. Experiment setup

To replicate web browser actions when a user visits a website, we use automated Firefox 67.0.1 to randomly visit the websites in our list in headless mode as discussed in prior works [9], [2] . This is a clean instance without any ad or pop-up blockers. We, however, install a plugin to export HTTP Archive (HAR) objects from each visited website. We store these HARs in a PostgreSQL database as JSON objects. Each browsing session uses a randomly selected configuration tuple of the form (domain, recursive resolver, DNS type [Do53, DoT, DoH]) to measure the QoE impact of each of the DNS protocols from the 11 public recursive resolvers from Four DNS providers; Adguard, CleanBrowsing, Cloudflare and Quad9. Of the four resolvers, two (Cloudflare and Quad9) negotiate TLS1.3 while CleanBrowsing and AdGuard negotiate TLS1.2

Firefox web browser natively supports Do53 and DoH. On the other hand, DoT has to be configured on the user's machine outside the browser. As such, we use *Stubby* for DoT resolution, a stub resolver based on the *getdns* library. *Stubby* listens on a loopback address and responds to Do53 queries. All DNS queries received by *Stubby* are then sent out to a configured recursive resolver over DoT. We modify /etc/resolv.conf on our measurement systems to point to the loopback address served by *Stubby*. This forces all DNS queries initiated by Firefox to be sent over DoT. This randomisation was done to avoid the potential effect of a query warming the resolver's cache for subsequent queries from the other protocols tested.

This measurements study was done in two blocks; 1 March 2020 to 30 August 2020 and 1 June 2021 to 17 June 2021) from 13 end-user vantage points located in 7 countries under three network conditions, 4G, Eduroam, wired campus network. We conducted the measurements continuously, with no delays between successive page loads. The researchers had access to the vantage points. We ran the measurements on i5 computers with 8GB of RAM running the Ubuntu 18.04 desktop version.

B. Metrics

This study aimed to understand the impact of DNS filtering on browsing Quality of Experience (QoE). The study considered network-level and browser-level metrics. These metrics are latency, DNS response time (in this paper referred to as DRT), DNS success and failure rates and page load time (PLT).

1) Latency: Several studies have pointed out that African networks suffer high latencies. Recent studies [18], [19], [20] have attributed these latencies to suboptimal routing, lack of peering and cache sharing. Other studies have attributed these latencies to offshore hosting and misconfiguration of DNS. However, none of these works has looked at the impact of security protocols on latency in the region. Latency determines the kind of applications that can run on affected networks. Therefore, it is important to understand how secure DNS protocols affect QoE to inform Internet users what

applications may run on a given network condition. Also, it is important to show which DNS providers respond with reasonable latency. This would aid users in the choice of DNS recursive resolvers. We conduct ping measurements to each of the resolvers and calculate the median RTT for each latency measurement.

2) DNS Resolution Time: DNS query response time is one of the major factors that affect the speed of page rendering in the browser. A web page normally contains several objects fetched from different servers. In this study, we measured DNS resolution time firstly for the main page. After that, we collected all the unique domains for components (i.e. images, JavaScript, CSS, among others) for each domain and measured their respective DNS Response time. We use *getdns* and *libcurl* C libraries to issue Do53, DoT, and DoH queries. *Getdns* provides an API that allows developers to perform DNS Do53 and DoT requests using different programming languages. Libcurl supports POST requests to be sent via HTTPS. This capability enables us to measure DoH response time. We could have gotten the DNS response times from the collected HARs; however, we noted that some of the timings were not correct and decided to use the *getdns*. It is important to note that the DNS responses were not cached by the browser used in the measurements to ensure that the subsequent transaction is not affected by the cache.

3) Page Load Time: Page load time is an important metric of browser-based QoE. It represents the time a user has to wait before the page is loaded in a browser. In this study, Firefox was used in headless mode to visit a set of websites. We collect HAR files in JSON format for each website containing timing information, including blocking information, proxy negotiation, DNS lookup, TCP handshake, SSL, Requests, Waiting and Content download. From the HAR files, we record the *onLoad* timing - the time taken to load the page together with its components completely.

C. Analysis

We use descriptive statistics to explore the data. We then apply Shapiro to test normality. Finally, we conduct a pairwise comparison of the DNS filters from the same provider using a T-test to explain their relationship. For example, Cloudflare provides two filters; security (CFS) and family (CFF) and one non-filter resolver (CFN) each of which provides three DNS protocols (Do53, DoH, DoT). In the study, we are interested in identical comparisons, Do53 against Do53, DoT against DoT and DoH against DoH. This gives us nine pairwise tuples {(CFN_Do53, CFF_Do53), (CFN_Do53, CFS_Do53), (CFF_Do53, CFS_Do53), (CFN_DoH, CFF_DoH), (CFN_DoH, CFS_DoH), (CFF_DoH, CFS_DoH), (CFN_DoT, CFF_DoT), (CFN_DoT, CFS_DoT), (CFF_DoT, CFS_DoT)) } on which we perform T-test.

III. Results

In total, we managed to successfully download and save $492,977$ HTTP Archive Record (HAR) files from which we obtain and analyse the page load times (PLT). Each successfully saved HAR had a number of objects, which we measured independently for DNS response time (DRT). This yielded $3,427,808$ unique domains, which translates to, on average, ≈ 7 domains referenced by a single HAR file.

A. Latency

We used ICMP ping to measure latency. Each successfully saved HAR file was accompanied by five ping measurements to the recursive resolver. This metric explains the differences in the DNS response times and page load times between resolvers from the same provider and between resolvers from different providers. As expected, we generally observe lower latencies to local resolvers provided by the Internet Service Providers. However, for some ISPs such as Telekom Networks Malawi, MTN Zambia and MTN Nigeria, we noted higher latencies than public resolvers such as Quad9 and Cloudflare. We posit that this might be the case under suboptimal routing. Also, this may be the case when ISPs choose not so highly cached DNS resolvers.

Observing from the network conditions' point of view, we find the lowest latency on wired (median RTT ≈ 87ms) network followed by Eduroam (median RTT ≈ 92ms) with the higher latencies observed under 4G (median RTT ≈ 446ms). We further observed differences in latencies under 4G; some countries had lower latencies than others. Comparing different resolvers, results indicate higher latencies to AdGuard resolvers with a minimum RTT of ≈ 750ms. In general, the latency results suggest that the resolvers from the same DNS providers are colocated.

B. DNS resolution Delay

DNS response time is one of the sources of delay in any online transaction that fetches resources from a remote location. A web transaction, in particular, comprises multiple name resolutions for page components such as images, scripts and cross-site components. This section presents summaries of DNS response times from all the measured resolvers, grouped by DNS provider and the network conditions. Due to space limitation, we focus our reporting on results from Cloudflare representing the fastest DNS provider observed in this study.

Figures 1, 2 and 3 show Cumulative Distribution Functions (CDFs) of DNS response times for the protocols and filters from Cloudflare. As expected, we note that Do53-based filters perform better than their corresponding DoE-based filters. This makes sense, considering the extra latency brought by the TLS handshakes. Comparing DoH and DoT from each resolver, we note that generally, DoT has higher DNS response times than DoH except for Cloudflare resolvers which show almost no difference. Also, we note in the 4G results (Figure 1) that the public Do53 perform better than the local Do53 provided by the Internet Service Providers. We note substantial differences in response times between filters and their respective protocols from three (Cloudflare, Adguard and Quad 9), with minimal differences noted from CleanBrowsing's filters. Comparing filters and non-filters, we note that the filters, especially DoH-based filters, provide lower response times than their non-filtered counterparts.

Comparably, Cloudflare resolvers perform better than the rest of the resolvers. Prior works [9], [21] have attributed this to the fact that Cloudflare resolvers do not support EDNS. In this work, we did not validate this claim. We also argue that Cloudflare has multiple points of presence in the region. This agrees with the latency results in which Adguard has the highest RTTs. Traceroute results show that Adguard resolvers are not present in Africa, hence the higher RTTs. When compared against each other, security filters outperform family filters. This pattern is helpful as it could inform the users of protocols or filters that would give them the best Quality of Experience.

Of peculiar notice is the performance of Quad9's DoT, which is consistently poorer regardless of network conditions. Prior works [9], [7], [2] have reported this observation. However, we have not engaged the provider to report or seek explanations as at writing this paper.

So far, we have observed using descriptive statistics that there are differences between resolvers from the same provider in terms of DNS response times. The question we ask is, are these differences significant? To answer this question, we conducted a T-test between the same protocols from different resolvers. Generally, we find that the results agree with the descriptive statistics as presented by the CDFs such as those presented in Figures 1, 2 and 3. We observe that the difference between filters from the same provider is mostly significant across recursive resolvers ($p < 0.001$) except for some fewer cases [(AGAd, AGF), (AGN, AGAd), (CBA, CBS), (CFF, CFS)] where the difference is not statistically significant.

On the other hand, we observe significant differences between DoE-based filters. Of the providers, Adguard and Quad9 show substantial differences (depicted by larger t values) than Cloudflare and CleanBrowsing. When we compare the filters, we note significant differences between the non-filter DoE resolvers and filtered resolvers. However, we note marginal differences between the filters (i.e. substantial differences between (CFN, CFS) and (CFN, CFF) and marginal differences between CFS and CFF). We also note that, under better network conditions, DoT filters are not statistically significant.

C. Page Load Times (PLT)

Pageload time is a more direct indication of how users experience web browsing. We have already seen the differences in query response times among the various DNS protocols under different network types across African vantage points. This section shows how the choice of filters and DNS providers would impact the quality of the browsing experience. We begin by comparing different filters with the local, non-filtered recursive resolver. This would inform the users of the cost they are likely to incur should they prefer open, public DoE filtering services to the Do53 service provided by their ISPs. Finally, we will compare the DoE-based filters with their Do53 counterparts.

Generally, we note a similar pattern between the latency, response time and page load time results. This is unsurprising considering that, to a greater extent, TLS-based security protocols are mainly determined by latency due to the extra overhead incurred during TLS handshake. Figure 4 shows the median page load time differences between public DNS providers and a local DNS recursive resolver. The difference is calculated by taking the median page load time for a website/user using one public, filter-enabled resolver minus the median page load time of the same website/user using a local, unfiltered resolver. Therefore, the difference is indicative of the extra cost a user would bear when using secure DNS protocols provided by public DNS resolvers compared to default Do53. From this Figure, we note that DoT performs better than DoH except for two cases (Cloudflare no filter and Quad9 no filter). Q9N's DoT displays extreme results with a mean page load difference of about seven seconds, concurring with the DNS response time results.

When we compare the providers, Cloudflare and CleanBrowsing fare consistently better than AdGuard and Quad9 with a page load difference of $\approx$ 2 seconds. We expected Cloudflare to perform comparably to Quad9, considering that both have multiple points of presence in Africa. We think that Quad9's DoE has some protocol design or infrastructural issues such as caching.

We also use Figure 4 to analyse the performance differences among DoE filters from the same provider with respect to the filter's Do53 performance. We note marginal differences between DoT and DoH-based filters with a median page load difference of up to 2 seconds except for Quad9's DoT, which we have already discussed in previous paragraphs. However, another aim of this study is to see whether these differences are statistically significant. We use a T-test to investigate the similarity and differences between filters and protocols from the same provider. We observe significant differences in the performance of Adguard, Cloudflare and Quad9 resolvers. Cloudflare (See Table I) generally sows significant differences in page load times except for DoT under wired network, suggesting that DoT's performance between CF's filters is not different under better network conditions. CleanBrowsing, however, does not show any significant differences between its resolvers across network conditions. This is in contrast to the DNS response time T-test results. CleanBrowsing's filters are not new, suggesting that they may have higher cache hits in Africa. On the other hand, Cloudflare's and Quad9's filters are new, and users and ISP's are yet to cache them hence the substantial difference. Adguard's performance is attached to the long distance from the vantage points to its points of presence which, from the latency measurements, indicate that they are situated offshore.

IV. Discussion and Implications

Thus far, we have presented results indicating significant differences in DNS response time and page load times exhibited by filter-enabled resolvers from the same public DNS provider. These differences are observed from all the measured network conditions; 4G, Eduroam and Campus wired broadband networks. The key role of DNS-based filtering

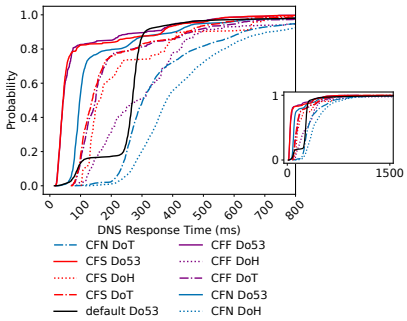

Fig. 1: DNS response time CDF for Cloudflare filters under 4G

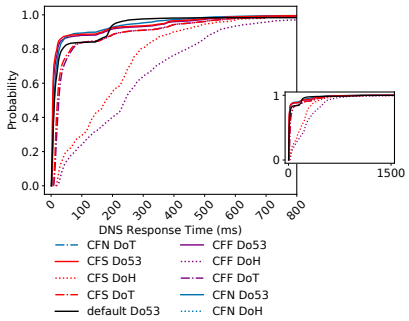

Fig. 2: DNS response time CDF for Cloudflare filters under Eduroam

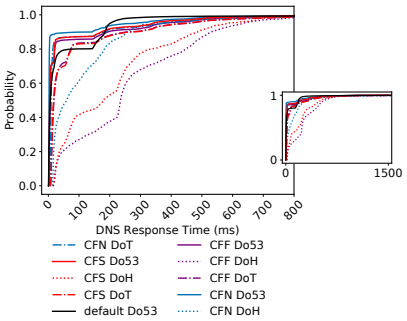

Fig. 3: DNS response time CDF for Cloudflare filters under wired network

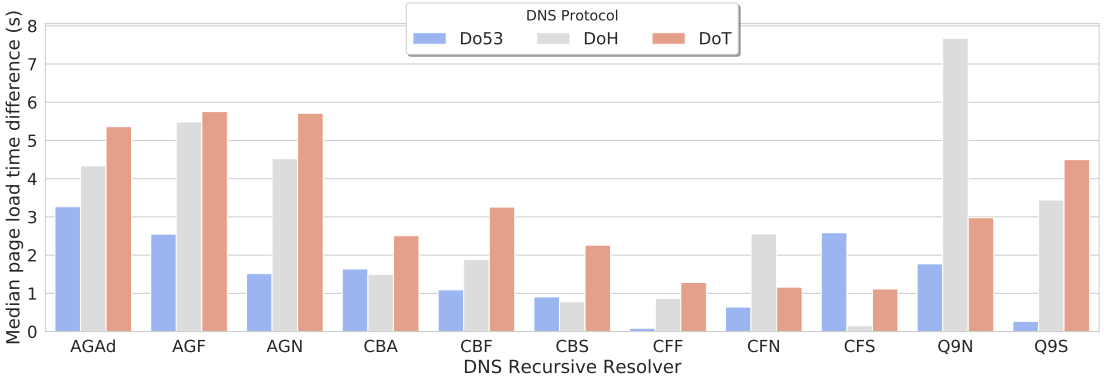

Fig. 4: Mean page load time difference between public and local recursive resolver

Pairwise PLT T-test-Cloudflare	Wired Network	Eduroam	4G
(CFN_Do53, CFF_Do53)	(t=14.931, p=0.000)*	(t=7.287, p=0.000)*	(t=6.928, p=0.000)*
(CFN_Do53, CFS_Do53)	(t=14.615, p=0.000)*	(t=7.473, p=0.000)*	(t=6.150, p=0.000)*
(CFF_Do53, CFS_Do53)	(t=-0.316, p=0.752)	(t=0.191, p=0.849)	(t=-0.549, p=0.584)
(CFN_DoH, CFF_DoH)	(t=2.651, p=0.008)*	(t=3.015, p=0.003)*	(t=2.090, p=0.036)*
(CFN_DoH, CFS_DoH)	(t=2.857, p=0.004)*	(t=2.809, p=0.005)*	(t=1.407, p=0.160)
(CFF_DoH, CFS_DoH)	(t=0.207, p=0.836)	(t=-0.244, p=0.807)	(t=-0.500, p=0.617)
(CFN_DoT, CFF_DoT)	(t=-0.432, p=0.666)	(t=2.234, p=0.026)*	(t=6.225, p=0.000)*
(CFN_DoT, CFS_DoT)	(t=0.318, p=0.750)	(t=3.210, p=0.001)*	(t=5.408, p=0.000)*
(CFF_DoT, CFS_DoT)	(t=0.766, p=0.443)	(t=1.136, p=0.256)	(t=-0.371, p=0.711)

TABLE I: T-tests for Cloudflare's Page load time

is to protect Internet users from malware, adware, phishing, cyberbullying and pornography. The results have also shown that DNS-based filters generally outperform their non-filter counterparts, implying that their usage would improve the Quality of Experience. Comparing the DNS providers, Adguard and Quad9 perform more poorly than Cloudflare and CleanBrowsing. Cloudflare performs consistently better across all network conditions. From these findings, we offer the following suggestions as possible remedies.

A. Implement local and regional DoE Infrastructure

ISPs widely use DNS level filtering as a value-added service to their customers to block malware, enforce parental controls, and prevent different cyber attacks. The problem with the Do53-based filtering was its invasive nature into the privacy of the subscribers described in the RFC [16] and various DNS attacks. The coming of the standard DNS privacy protocols is a relief to many security-conscious Internet subscribers. The limiting factor, however, could be the performance overhead incurred when using public resolvers. Also, other subscribers would not be comfortable using third-party DNS providers. This study and other prior works suggest that the closer the resolvers are to the end-user, the better the Quality of Experience. Therefore, we recommend that the ISPs and Network Operators implement DoE services. This would reduce the latency overhead and eventually improve QoE.

B. Offer configurable Quality of Protection to Internet Users

Internet is costly in edge networks. Because of this, paternalistic or stupid user implementation of Internet security services may negatively impact some users from these networks. On the other hand, the configuration of Internet security services is not straightforward [22] imposing security configuration overhead on the users. Consequently, most users have developed poor mental models around security, including DNS service, and they do not find the motivation to configure security on their Internet access devices. We are aware of recommendations by researchers to optimise secure DNS. Deccio C. and Davis J. [23], connection-oriented DNS by Zhu, *et al.* [24] proposed the usage of TCP Fast Open (TFO) and TLSv1.3. Hounsel *et al.* [9] propose opportunistic partial responses, wire caching and disabling of EDNS Client-Subnet.

One possibility is to introduce an integrated, easy-to-use cost-aware Internet security configuration framework that will enable users to choose their desired level of security, such as choosing the type of DNS filters in this case.

Finally, the results from this study enable both users and ISPs to make better DNS choices based on the measurement data and based on the trust they have in the DNS provider. The results also inform the DNS providers on the possible improvements and expansion of their services in Africa.

V. Conclusion and future work

This paper investigated the QoE impact of public Do53 and DoE-based filtering from African vantage points. The study has shown that users who use DNS filters would experience a better QoE. In some cases, the study has shown that DoE-based filtering performs even better than Do53-based filters. The results from this study assist Internet Service providers and Internet users to make sound decisions when choosing the DoE-based filters to implement. The choice of DNS filters would improve the Quality of Protection and Experience.

Acknowledgement

The authors are grateful for the financial support received from the Hasso Plattner Institute (HPI) through the HPI Research School at the University of Cape Town.

References

[1] Mockapetris, P. Domain Names - Concepts and Facilities. RFC 1034, IETF (1987). URL https://www.ietf.org/rfc/rfc1034.txt.

[2] Mbewe, E. S. & Chavula, J. On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters. In Zitouni, R. *et al.* (eds.) *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 361, 289–304 (Springer International Publishing, Cham, 2021).

[3] Hu, Z. *et al.* Specification for DNS over Transport Layer Security (dotls). RFC 7858, IETF (2016). URL https://tools.ietf.org/html/rfc7858.

[4] McManus, P. H. . P. DNS Queries over HTTPS (DoH). RFC 8484, IETF (2018). URL https://tools.ietf.org/html/rfc8484.

[5] dnscrypt.info. DNSCrypt version 2 protocol specification. URL https://dnscrypt.info/protocol.

[7] Lu, C. *et al.* An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? *Proceedings of the Internet Measurement Conference* (2019).

[6] dnscurve.org. DNScurve: Usable security for DNS. URL https://dnscurve.org/.

[8] Böttger, T. *et al.* An Empirical Study of the Cost of DNS-over-HTTPS. In *Proceedings of the Internet Measurement Conference*, IMC '19, 15–21 (Association for Computing Machinery, New York, NY, USA, 2019). URL https://doi.org/10.1145/3355369.3355575.

[9] Hounsel, A., Borgolte, K., Schmitt, P., Holland, J. & Feamster, N. Analyzing the costs (and benefits) of DNS, DoT, and DoH for the modern web. *Proceedings of the Applied Networking Research Workshop* (2019).

[10] Hounsel, A., Borgolte, K., Schmitt, P., Holland, J. & Feamster, N. Comparing the effects of DNS, DoT, and DoH on Web Performance. In *Proceedings of The Web Conference 2020*, WWW '20, 562–572 (Association for Computing Machinery, New York, NY, USA, 2020). URL https://doi.org/10.1145/3366423.3380139.

[11] Hoang, N. P., Lin, I., Ghavamnia, S. & Polychronakis, M. K-resolver: Towards Decentralizing Encrypted DNS Resolution. *ArXiv* **abs/2001.08901** (2020).

[12] Hounsel, A., Borgolte, K., Schmitt, P. & Feamster, N. D-DNS: Towards Re-Decentralizing the DNS. URL https://arxiv.org/abs/2002.09055. 2002.09055.

[13] Stalmans, E. & Irwin, B. A framework for DNS based detection and mitigation of malware infections on a network. In *2011 Information Security for South Africa*, 1–8 (2011).

[14] Alieyan, K. *et al.* DNS rule-based schema to botnet detection. *Enterprise Information Systems* **0**, 1–20 (2019). URL https://doi.org/10.1080/17517575.2019.1644673.

[15] Singh, M., Singh, M. & Kaur, S. Issues and challenges in DNS based botnet detection: A survey. *Computers & Security* **86**, 28–52 (2019). URL http://www.sciencedirect.com/science/article/pii/S0167404819301117.

[16] Farrell, S. & Tschofenig, H. Pervasive Monitoring is an attack. RFC 7258, IETF (2014). URL https://tools.ietf.org/html/rfc7258.

[17] Livingood, J., Antonakakis, M., Sleigh, B. & Winfield, A. Centralized DNS over HTTPS (DoH) Implementation Issues and Risks. Draft, IETF (2019). URL https://tools.ietf.org/id/draft-livingood-doh-implementation-risks-issues-03.html.

[18] Calandro, E., Chavula, J. & Phokeer, A. Internet Development in Africa: A Content Use, Hosting and Distribution Perspective. In Mendy, G., Ouya, S., Dioum, I. & Thiaré, O. (eds.) *e-Infrastructure and e-Services for Developing Countries*, 131–141 (Springer International Publishing, Cham, 2019).

[19] Formoso, A., Chavula, J., Phokeer, A., Sathiaseelan, A. & Tyson, G. Deep diving into Africa's inter-country latencies. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2231–2239 (2018).

[20] Fanou, R. *et al.* Exploring and analysing the African Web ecosystem. *ACM Trans. Web* **12**, 22:1–22:26 (2018). URL http://doi.acm.org/10.1145/3213897.

[21] Knows, S. DNS-over-HTTPS performance (2019). URL https://www.samknows.com/blog/dns-over-https-performance.

[22] Borgolte, K. *et al.* How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem. *SSRN Electronic Journal* (2019).

[23] Deccio, C. & Davis, J. DNS Privacy in Practice and Preparation. In *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, CoNEXT '19, 138–143 (Association for Computing Machinery, New York, NY, USA, 2019). URL https://doi.org/10.1145/3359989.3365435.

[24] Zhu, L. *et al.* Connection-Oriented DNS to Improve Privacy and Security. In *2015 IEEE Symposium on Security and Privacy*, 171–186 (2015).

Enock Samuel Mbewe is a PhD candidate in the Computer Science at the University of Cape Town (UCT). His research is on configurable Internet security. In particular, his work investigates the use of a novel, cost-aware Internet security decision model to allow users, especially those with limited computing skills, to easily configure security options that can map to complex Internet security mechanisms to achieve Confidentiality, Integrity, Authentication and Privacy. He received MSc in Information Theory, Coding and Cryptography and a BSc in ICT from Mzuzu University, Malawi.

Josiah Chavula is a lecturer and researcher in Computer Science at the University of Cape Town. He received a PhD in Computer Science from UCT (2017), and an MSc in Networking and Internet Systems from Lancaster University (2011). His research focuses on performance of internet systems in Low Resource contexts.