Decentralization, Privacy and Performance for DNS

Rashna Kumar
Northwestern University
rashnakumar2024@u.northwestern.edu

Fabián E. Bustamante
Northwestern University
fabianb@cs.northwestern.edu

ABSTRACT

The Domain Name System (DNS) is both key determinant of a users' quality of experience (QoE) and privy to their tastes, preferences, and even the devices they own. Growing concern about user privacy and QoE has brought a number of alternative DNS techniques and services, from public DNS to encrypted and oblivious DNS. Today, a user choosing among these services and its few providers is forced to prioritize – aware of it or not – between web performance, privacy, reliability, and the potential for a centralized market and its consequences. We present *Ónoma*, a DNS resolver that addresses the concerns about DNS centralization without sacrificing privacy or QoE by sharding requests across alternative DNS services, placing these services in competition with each other, and pushing resolution to the network edge. Our preliminary evaluation shows the potential benefits of this approach across locales, with different DNS services, content providers, and content distribution networks.

KEYWORDS

ACM proceedings

ACM Reference Format:
Rashna Kumar and Fabián E. Bustamante. 2021. Decentralization, Privacy and Performance for DNS. In *SIGCOMM '21 Poster and Demo Sessions (SIGCOMM '21 Demos and Posters), August 23–27, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3472716.3472869

1 HAVE YOUR CAKE AND EAT IT TOO

Name services are critical for mapping logical to physical resources in distributed systems. The main service fulfilling this role for the Internet is the Domain Name System (DNS) [21]. Whenever a user accesses a server on the Internet – visiting a web page, posting on a social network or checking email, DNS translates the server's human-readable name to the addresses needed to route the request.

DNS is a key determinant of users' quality of experience (QoE) as, for instance, accessing any website today requires tens of DNS resolutions [9–11]. At the same time, the set of DNS requests issued by a user reveals much about their tastes, preferences, and even the devices they own and how they used them [1, 2, 8]. Clear text DNS requests can have a significant impact on privacy and security and, in certain parts of the world, on human rights [6, 13, 31].

Growing concerns about user privacy and quality of experience have served as motivation for a number of alternative DNS techniques and services, from public DNS to encrypted and oblivious DNS [19, 26, 26, 28]. Google Public DNS was announced in late 2009 promising better performance and higher reliability [15], while DNS over HTTPs (DoH), DNS over TLS (DoT), and Oblivious DNS are some of the latest proposals to make DNS more secure [20, 28]. While offering some valuable features, these DNS variants are supported by a handful of providers such as Google, Cloudflare or IBM, strengthening a problematic trend toward DNS centralization that has raised concerns about privacy, competition, resilience and Web QoE.

First, the use of encrypted DNS, while avoiding man-in-the-middle attacks, does not necessarily improve client's privacy as the DNS provider has access to the unencrypted request of millions of clients and is an easier target for a court order to release data in bulk [27]. Second, centralization in a small set of providers, particularly if they can erect barriers to competitive entrance, increases the risk of a captive market [3]. Third, part of the Internet's inherent resilience lies in its diversity – centralization leads to a clustering of multiple risks, from technical to economic ones [18] while increasing the potential impact of any single failure [14]. Last, while centralized DNS could offer better DNS response time, it may result in worst Web QoE. Despite some adoption of anycast [5, 12] and the promise of CDN-ISP collaborations [4, 23, 24, 30], many CDNs continue to rely on DNS for replica selection, building on the assumption that the location of a client's DNS resolver provides a good approximation to the client location. Centralized DNS breaks this assumption [22] since for specific locales a particular third-party DNS service may not have nearby servers to offer, negatively impacting both DNS resolution times and web QoE [22] for users of the many CDNs that continue to rely on DNS for replica selection.

Today, a user choosing among alternative DNS services, either their ISP's or one offered by a third-party, is forced to prioritize – aware of it or not – between web performance, privacy, reliability, and the potential for a centralized market and its consequences [3, 18, 25]. In this paper, we present *Ónoma*, an end-user DNS resolver designed to let users *have their cake and eat it too.*

These motivating trends and observations help shape the requirements of Ónoma.

- *Privacy*: Ónoma should be able to leverage the best techniques and services aimed at improving user privacy.
- *Performance*: Ónoma should offer performance comparable to that of the best performing services in the user's locale by incorporating state-of-art techniques to resolution times and users' QoE.
- *Decentralization*: Ónoma should let users avoid DNS centralizations, avoiding reliance on any single DNS service and putting alternative services in competition.

SIGCOMM '21 Demos and Posters, August 23–27, 2021, Virtual Event, USA
© 2021 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8629-6/21/08.
https://doi.org/10.1145/3472716.3472869

- *Dynamic*: Ónoma should be able to dynamically select the best DNS service providers in different locales.
- *Readily deployable*: Ónoma should be an easy-to-install, readily-deployable solution that bypasses the need for agreements and coordination between providers (CDNs, DNS or ISPs).

Ónoma (*i*) leverages the privacy and performance benefits of new DNS services while avoiding the risk of centralizing DNS information, (*ii*) improves resolution performance and resilience by sharding requests across multiple resolvers [7, 16, 17] and running resolution races [29], and (*iii*) reinstates the client-resolver proximity assumption CDNs rely on by changing the resolution process with the client-run resolver querying the CDN directly [22]. Figure 1 summarizes the model of the design for DNS query handling mechanism of Ónoma.

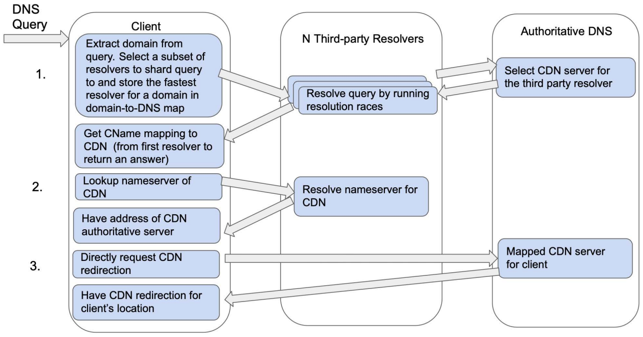

DNS Query
Client
N Third-party Resolvers
Authoritative DNS
1.
Extract domain from query. Select a subset of resolvers to shard query to and store the fastest resolver for a domain in domain-to-DNS map
Resolve query by running resolution races
Select CDN server for the third party resolver
Get CName mapping to CDN (from first resolver to return an answer)
2.
Lookup nameserver of CDN
Resolve nameserver for CDN
Have address of CDN authoritative server
3.
Directly request CDN redirection
Mapped CDN server for client
Have CDN redirection for client's location

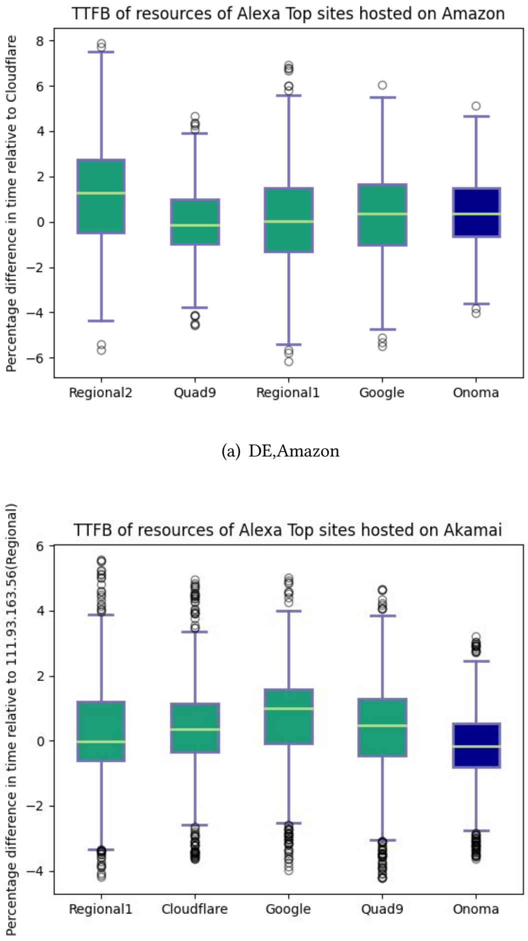
Figure 1: Client side system design of Ónoma showing the proposed alternative flow of DNS query handling.

We present preliminary evaluation results of Ónoma across geographic locales and with different DNS services, content providers, and CDNs. Our results show that by combining well-known techniques, one can avoid the privacy concerns with DNS request centralization without negatively impacting users QoE, and that while there may no be an ideal service for all clients in *all* places, an adaptive client-based solution can dynamically select the *best* service for *any* given location.

2 PRELIMINARY FINDINGS

To compare the benefits of Ónoma for QoE against other DNS services on different CDN service providers, we create a mapping of the resources of Top 50 Alexa regional sites and the CDNs they are hosted on. For each resource, we evaluate the performance of Ónoma across popular CDN service providers, i.e., Akamai, Amazon and Fastly, in each selected locales using the time-to-first-byte (TTFB) results collected from the measurements. We set up the evaluation measurements in the selected locations using VPN services.

Figure 2 shows the performance of individual, public DoH and DNS resolvers in each country and using Ónoma, relative to the best DNS service across different CDNs and countries. From the figure, we see that the performance of Ónoma is either best, or at a comparable position with the average of the public DNS services. We see significant performance improvement with content hosted on Amazon in Germany and with content hosted on Akamai in India.



(a) DE,Amazon

(b) IN,Akamai

Figure 2: Performance of individual, public DoH and DNS resolvers in each country and using Ónoma, relative to the best DNS service across different CDNs and countries.

Ónoma gives consistently lower inter-quartile range (IQR) for most cases and average performance of Ónoma is better than the best Service for most CDN, country combinations or at least comparable to all the DNS services tested for that locale.

3 CONCLUSION AND FUTURE WORK

We present Ónoma, a new client-based resolver that addresses the challenges of centralization without impacting users' QoE. Our preliminary results show the performance benefits of Ónoma in different locales and across DNS services, content providers and CDNs.

We are exploring different approaches to dynamically adjust the tradeoffs between privacy, performance and centralization based on measurements and user feedback, and casting part of the challenge as a differential privacy problem.

REFERENCES

[1] 2014. https://theintercept.com/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/

[2] 2015. https://leaksource.files.wordpress.com/2015/02/nsas-morecowbell-knell-for-dns.pdf

[3] 2020. Consolidation in the Internet Economy. https://future.internetsociety.org/2019/

[4] R. Alimi, R. Penno, and Y. Yang. 2011. *ALTO Protocol.* Technical Report RFC 7285. IETF.

[5] H.A. Alzoubi, S. Lee, M. Rabinovich, and J.V. Merwe O. Spatscheck. 2008. Anycast CDNS revisited.

[6] Anonymous. 2012. The Collateral Damage of Internet Censorship by DNS Injection. (July 2012).

[7] Jari Arkko, Martin Thomson, and Ted Hardie. 2020. *Selecting Resolvers from a Set of Distributed DNS Resolvers.* Internet-Draft. Internet Engineering Task Force.

[8] Stephane Bortzmeyer. 2015. *DNS Privacy Considerations.* RFC 7626. IETF.

[9] Timm Bottger, Felix Cuadrado, Gianni Antichi, Elder Leao Fernandes, Garth Tyson, Igancio Castro, and Steve Uhlig. 2019. An Empirical Study of the Cost of DNS-over-HTTPS.

[10] Ilker Nadi Bozkurt, Anthony Aguirre, Balakrishnan Chandrasekaran, P. Brighten Godfrey, Gregory Laughlin, Bruce Maggs, and Ankit Singla. 2017. Why is the Internet so slow?!

[11] Michael Butkiewicz, Harsha V. Madhyastha, and Vyas Sekar. 2011. Understanding Website Complexity: Measurements, Metrics, and Implications.

[12] M. Calder, A. Flavel, Ethan Katz-Bassett, Ratul Mahajan, and J. Padhye. 2015. Analyzing the performance of an anycast CDN.

[13] Mariengracia Chirinos, Andrés Azpúrua, Leonid Evdokimov, and Maria Xynou. 2016. The State of Internet Censorship in Venezuela. Open Observatory of Network Interference (OONI) Blog. https://ooni.org/post/venezuela-internet-censorship/.

[14] David Coldewey. 2020. Cloudflare DNS goes down, taking a large piece of the Internet with it. TechCrunch Blog. http://tcrn.ch/3pbDJzL

[15] Google. 2009. Introducing Google Public DNS. Google Code Blog. http://googlecode.blogspot.com/2009/12/introducing-google-public-dns-new-dns.html

[16] Nguyen Phong Hoang, Ivan Lin, Seyedhamed Ghavamnia, and Michalis Polychronakis. 2020. K-resolver: Towards Decentralizing Encrypted DNS Resolution. In *Proc. of MADWeb.*

[17] Austin Hounsel, Kevin Borgolte, Paul Schmitt, and Nick Feamster. 2020. D-DNS: Towards Re-Decentralizing the DNS. (February 2020).

[18] Geoff Huston. 2019. DNS Resolver Centrality. APNIC Blog. https://labs.apnic.net/?p=1260

[19] E. Kinnear, T. Pauly, C. Wood, and P. McManus. 2019. *Adaptive DNS: Improving Privacy and Name Resolution.* Network Working Group – Internet Draft. IETF.

[20] Chaoyi Lu, Baojun Liu anbd Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianping Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?

[21] Paul Mockapetris. 1987. *Domain Names – Concepts and Facilities.* RFC 1034. IETF.

[22] John Otto and Mario Sánchez John Rula Fabián E. Bustamante. 2012. Content delivery and the natural evolution of DNS: remote dns trends, performance issues and alternative solutions.

[23] I. Poese, B. Frank, G. Smaragdakis, S. Uhlig, A. Feldmann, and B. Maggs. 2012. Enabling Content-aware Traffic Engineering. (2012).

[24] Enric Pujol, Ingmar Poese, Johannes Zerwas, Georgios Smaragdakis, and Anja Feldmann. 2019. Steering hyper-giants' traffic at scale.

[25] Roxana Radu and Michael Hausding. 2020. Consolidation in the DNS resolver market – how much, how fast, how dangerous? *Journal of Cyber Policy* 5, 1 (February 2020), 46–64.

[26] Paul Schmitt, Anne Edmundson, Allison Manjin, and Nick Feamster. 2019. Oblivious DNS: Practical privacy for DNS queries. In *Proc. on Privacy Enhancing Technologies.*

[27] Jennifer Valentino-devries. 2019. Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies. https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html?smid=tw-nytimes&smtyp=cur

[28] Tanya Verna and Sudheesh Singanamalla. 2020. Improving DNS Privacy with Oblivious DoH in 1.1.1.1. CloudFlare Blog. https://blog.cloudflare.com/oblivious-dns/.

[29] Ashish Vulimiri, Oliver Michel, P. Brighten Godfrey, and Scott Shenker. 2012. More is Less: Reducing Latency via Redundancy.

[30] H. Xie, Y. R. Yang, A. Krishnamurthy, Y. G. Liu, and A. Silberschatz. 2008. P4P: Provider Portal for Applications.

[31] Maria Xynou, Arturo Filastò, Mahsa Alimardani, Sina Kouhi, Kyle Bowen, Vmon, and Amin Sabeti. 2017. Internet Censorship in Iran: Network Measurement Findings from 2014-2017. Open Observatory of Network Interference (OONI) Blog. https://ooni.org/post/iran-internet-censorship/