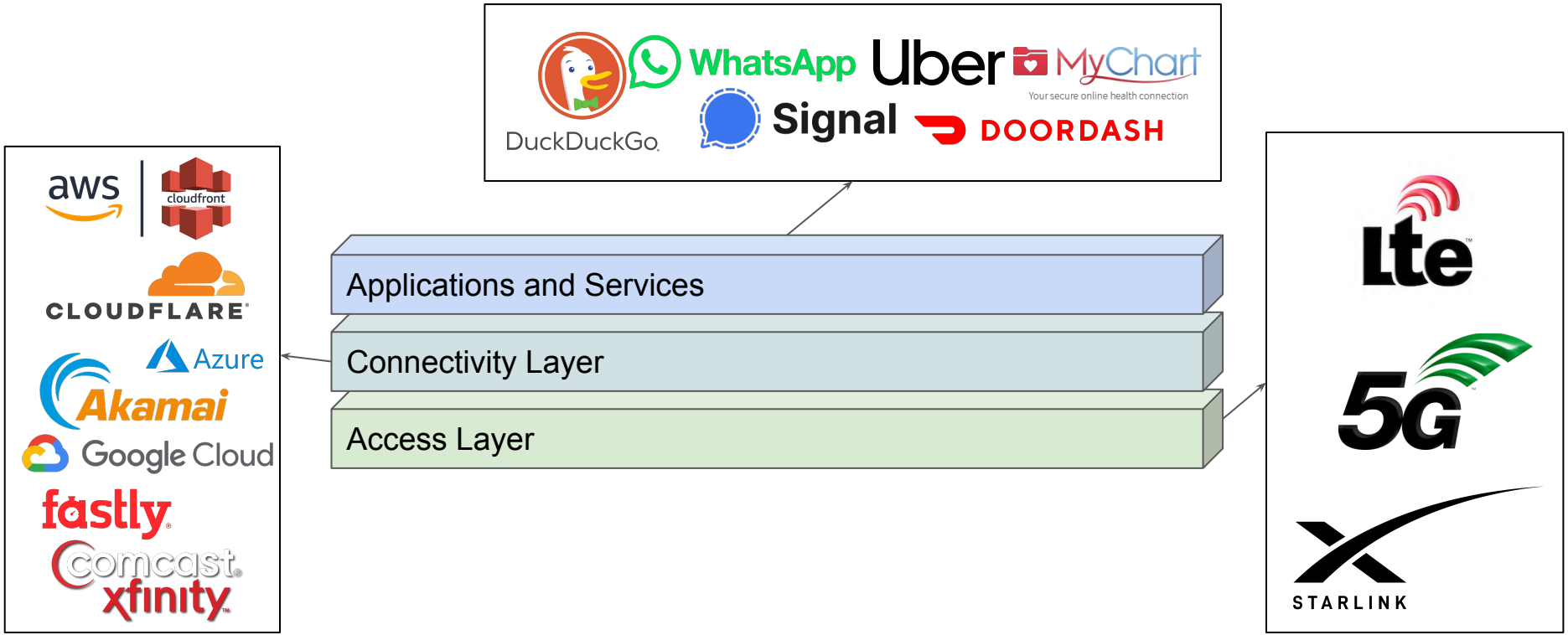
Distributing Trust in Critical Societal Scale Computing Infrastructure

Sudheesh Singanamalla

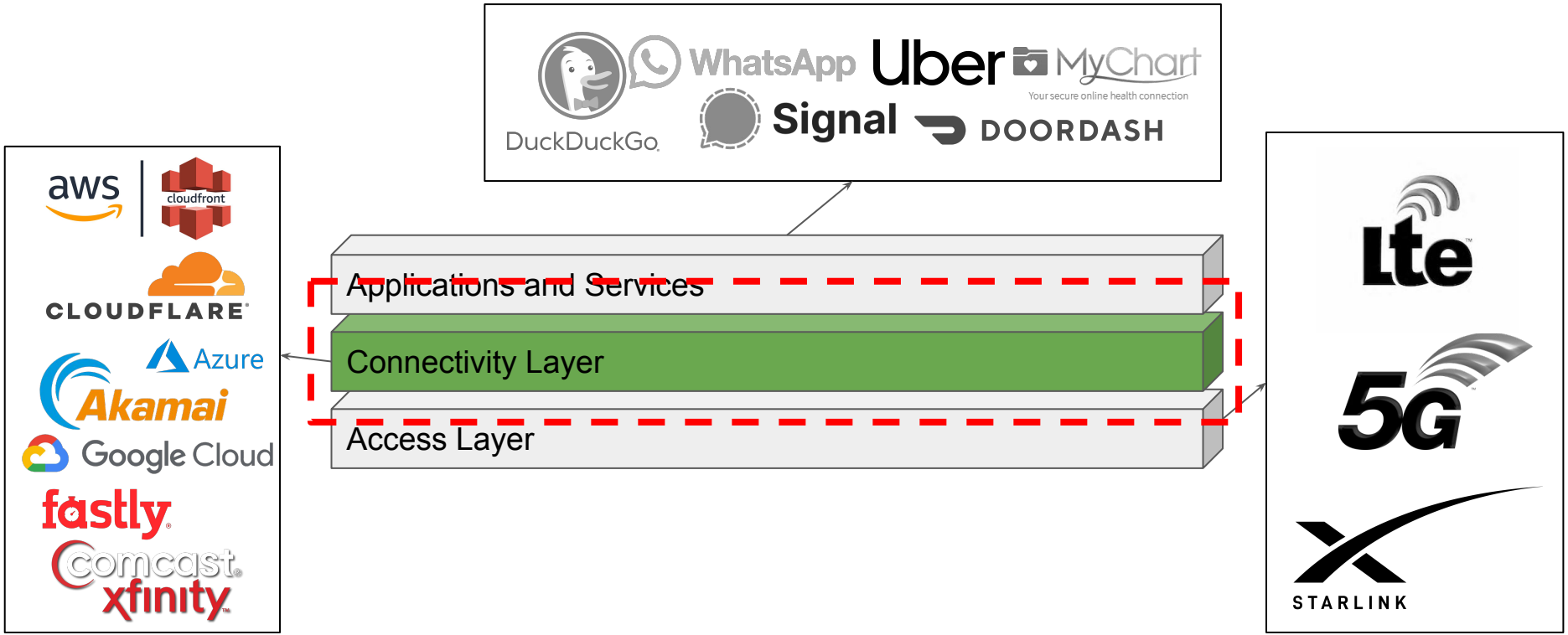
sudheesh@cs.washington.edu

PhD Candidate – University of Washington

Internet – Today's Critical Societal Infrastructure



Internet – Today's Critical Societal Infrastructure

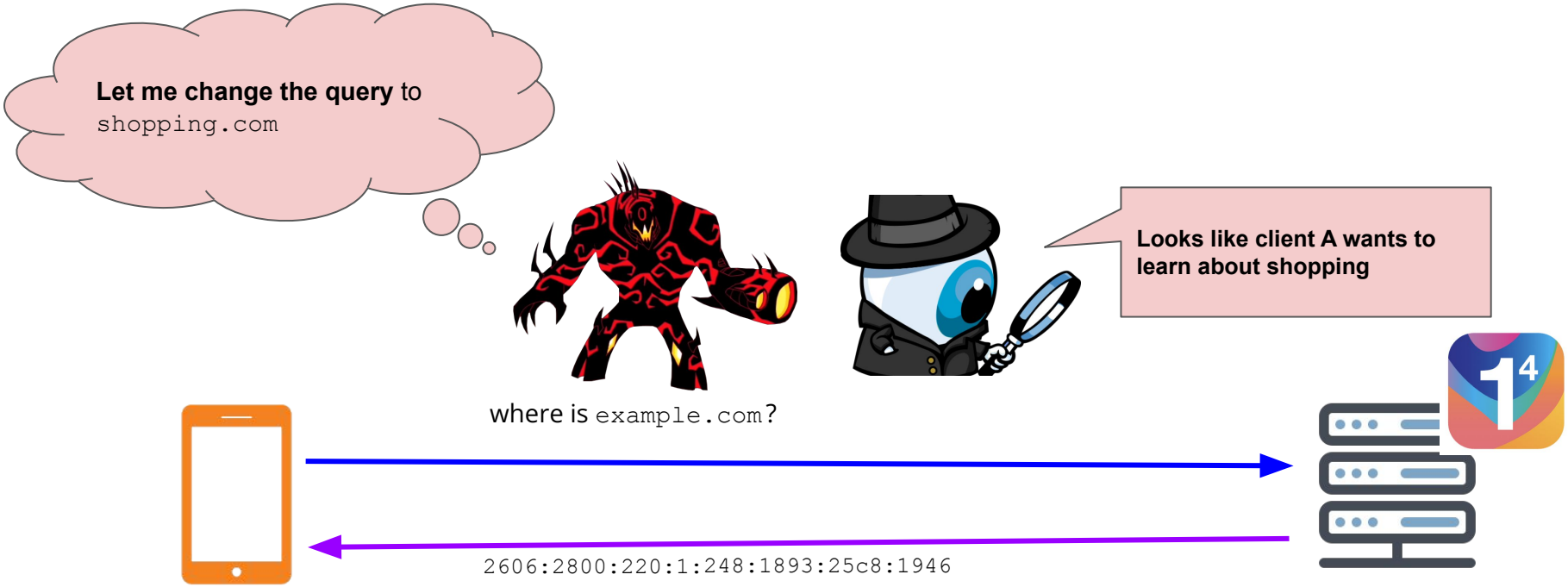


Trust In Today's Internet Infrastructure

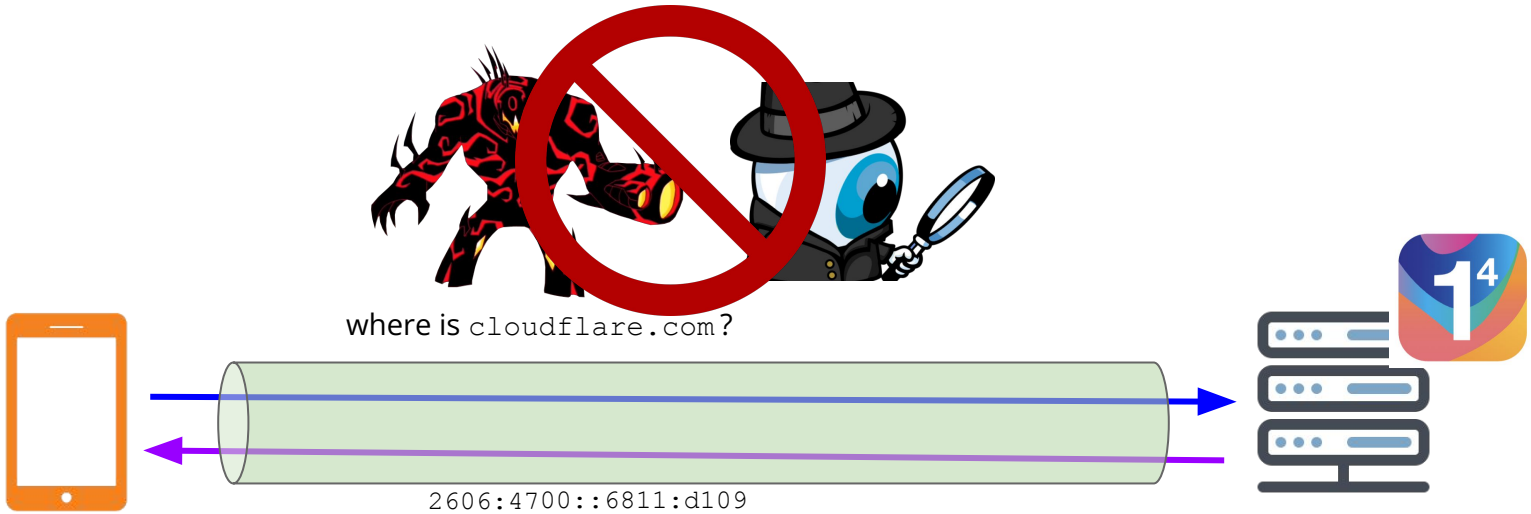
1. An increasing number of resources on the Internet today are served by a few large providers such as popular websites, or Content Delivery Networks
2. Users interact with a lot of hidden infrastructure – Routers, DNS resolvers, Network policy managers and Firewalls, etc..,
3. Burden on a few parties to maintain the security of the Internet today – Certificate Authorities and Certificate Transparency.

"While invisibility is the hallmark of effective infrastructures, Infrastructure often becomes visible upon breakdown" ~ Susan Leigh Star

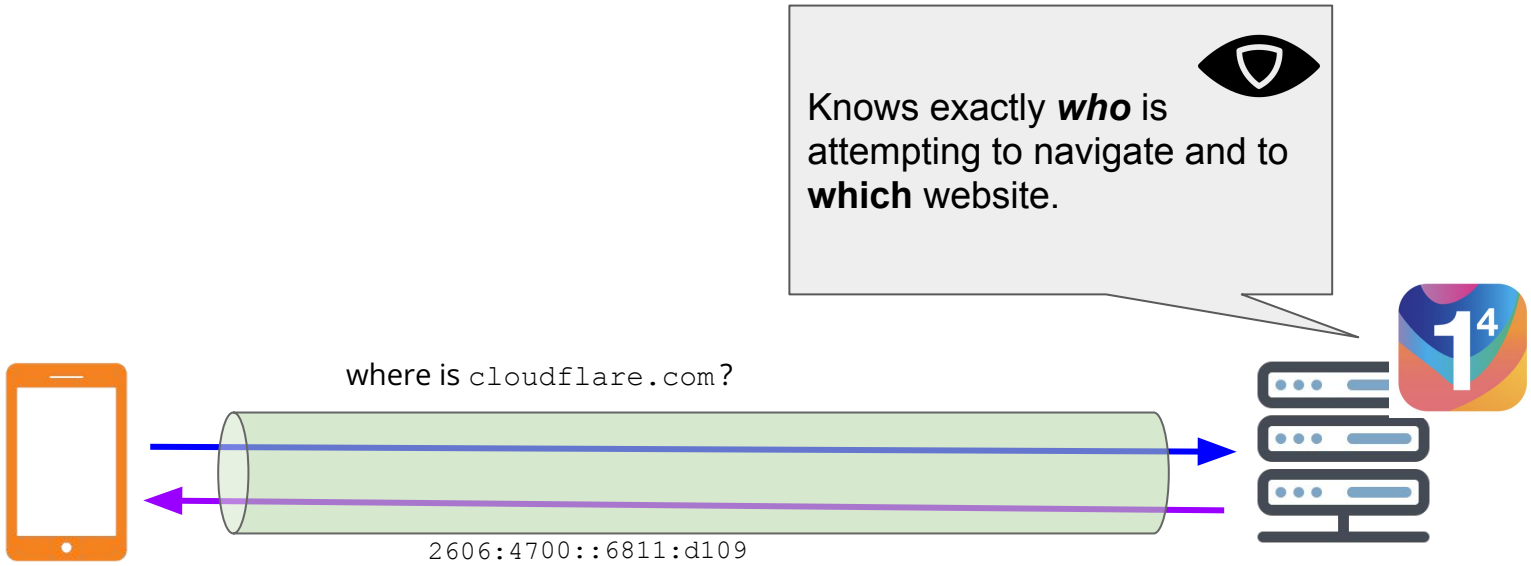
Plaintext DNS is Insecure – 92% of daily DNS Traffic to 1[4]



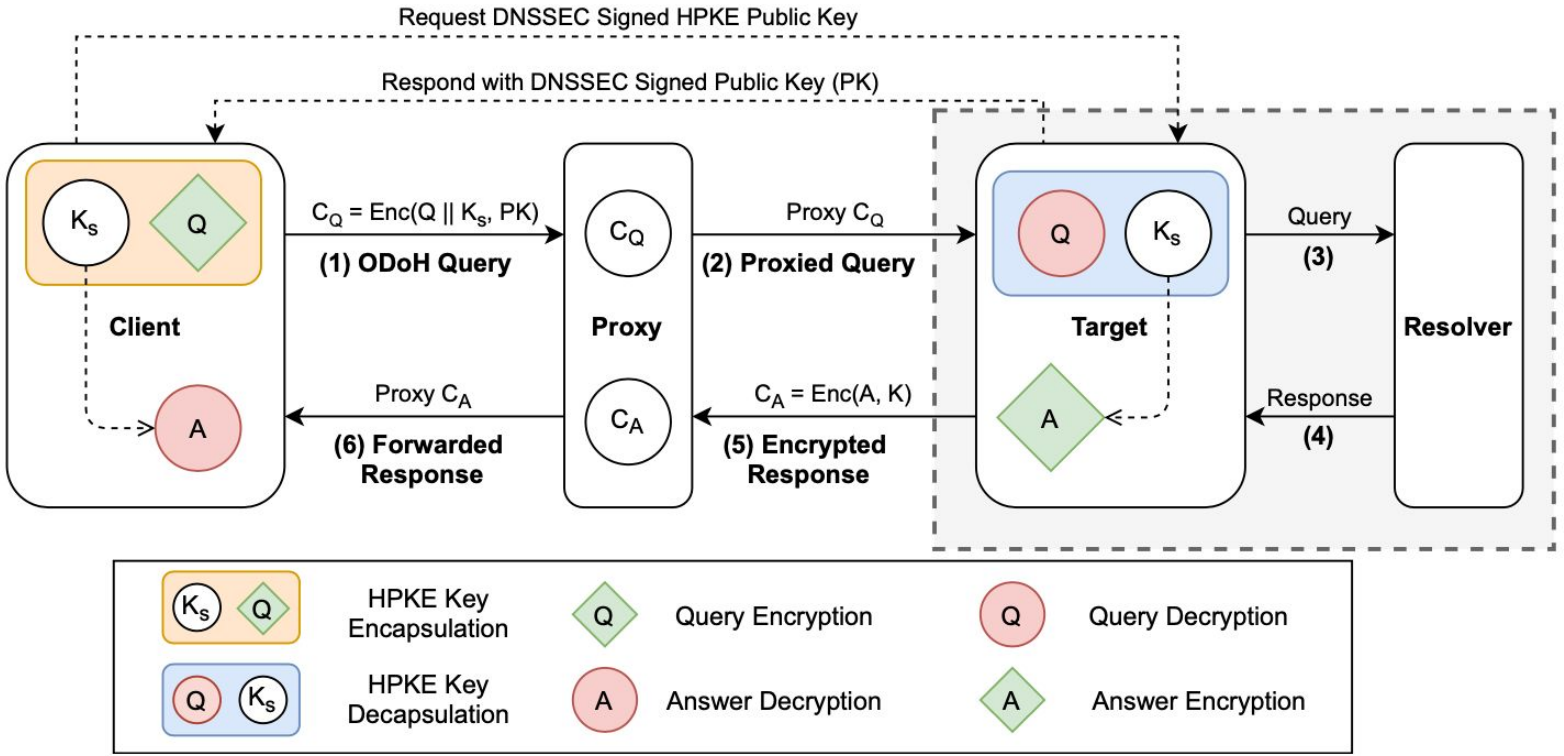
Secure Transports (DoH, DoT) Improve DNS Security



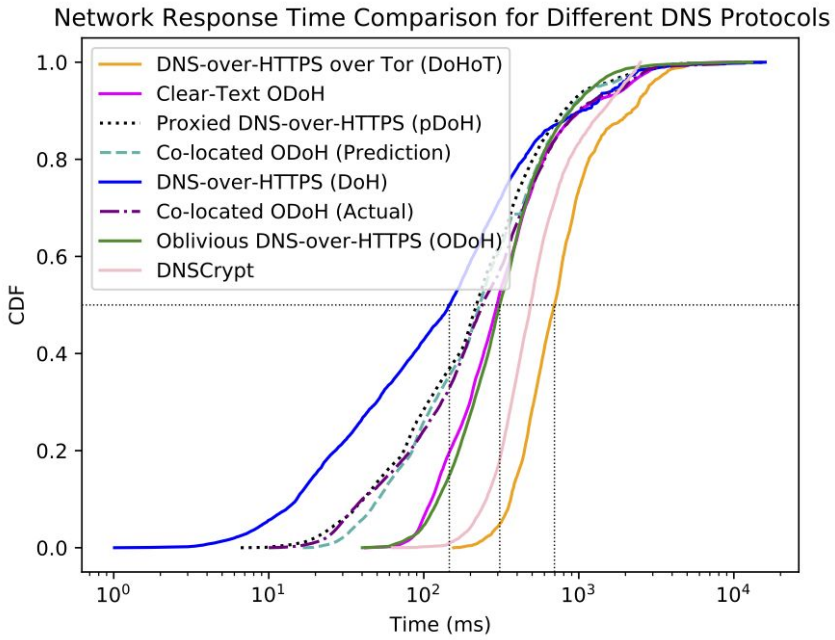
But … Raise A Key Privacy and Trust Issue



Oblivious DNS over HTTPS (ODoH)



Comparing ODoH with Other DNS Protocols

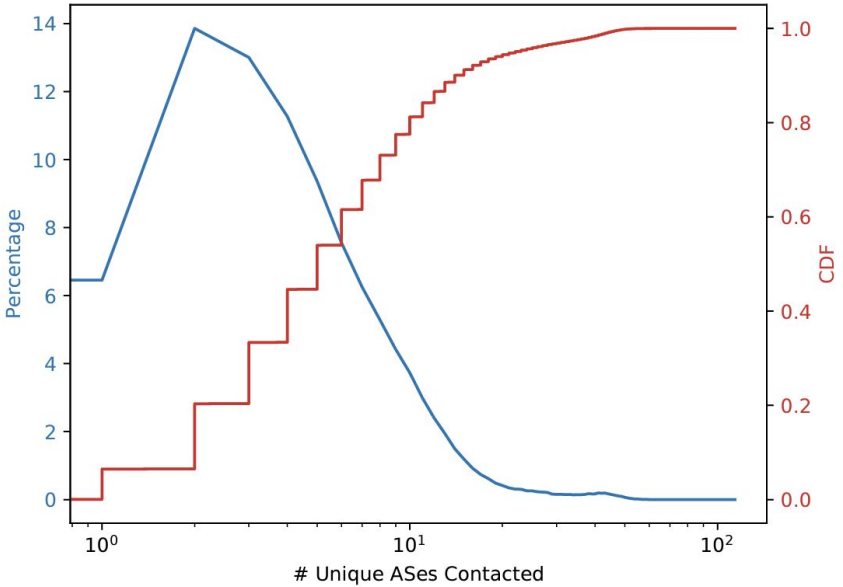


https://odoh.cloudflare-dns.com/

Protocol	Request Path	Security	Privacy
Plain DNS (Do53)	C → R	No	No
DNS over HTTPS (DoH)	C → R	Yes	No*
Proxied DoH	C → P → R	Yes	No
Oblivious DoH (ODoH)	**C → P → T → R**	**Yes**	**Yes**
Cleartext ODoH	C → P → T → R	Yes	No
Co-located ODoH	**C → P → (T+R)**	**Yes**	**Yes**
DNSCrypt	C → R	Yes	No*
Anonymous DNSCrypt	C → P → R	Yes	Yes
DoH over Tor (DoHoT)	C → Tor → R	Yes	Yes

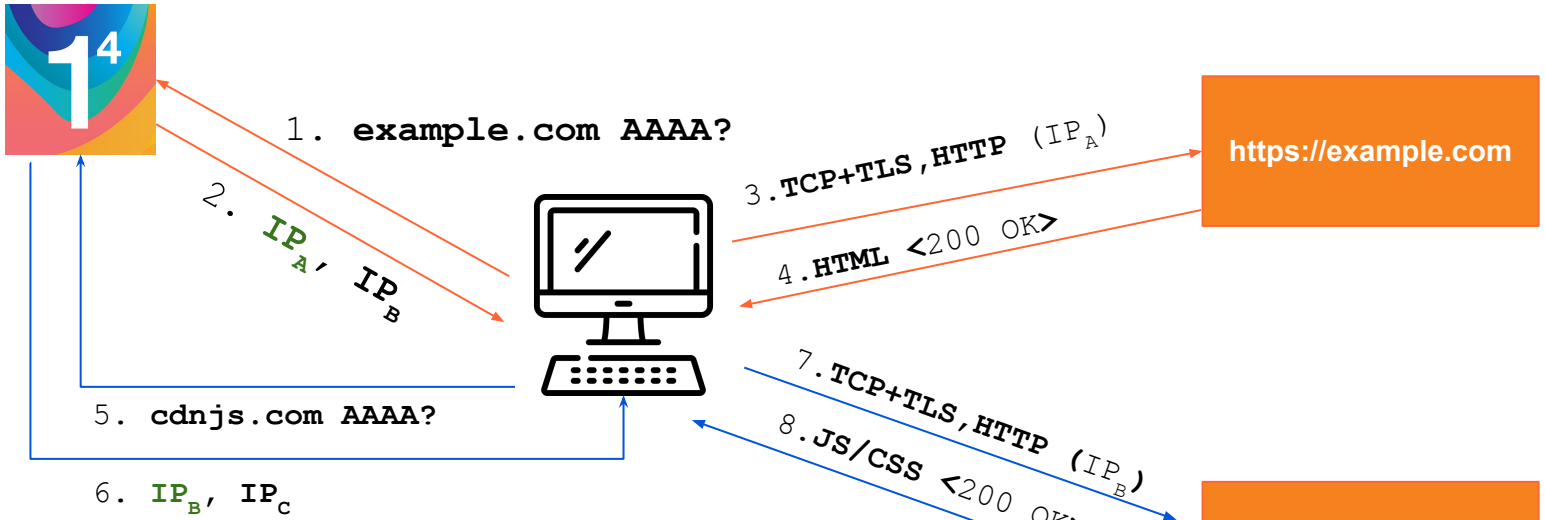
Where are our connections going during a page load?

Rank	AS Number	Org. Name	#Req	%
1	AS 15169	Google	7932198	22.10
2	AS 13335	Cloudflare	4937395	13.75
3	AS 16509	Amazon 02	3017176	8.40
4	AS 14618	Amazon AES	2019308	5.62
5	AS 54113	Fastly	1281402	3.57
6	AS 16625	Akamai AS	1087172	3.02
7	AS 32934	Facebook	998685	2.78
8	AS 20940	Akamai Intl. B.V.	583700	1.62
9	AS 16276	OVH SAS	548107	1.52
10	AS 24940	Hetzner Online GmbH	469293	1.30
Total				**63.68**



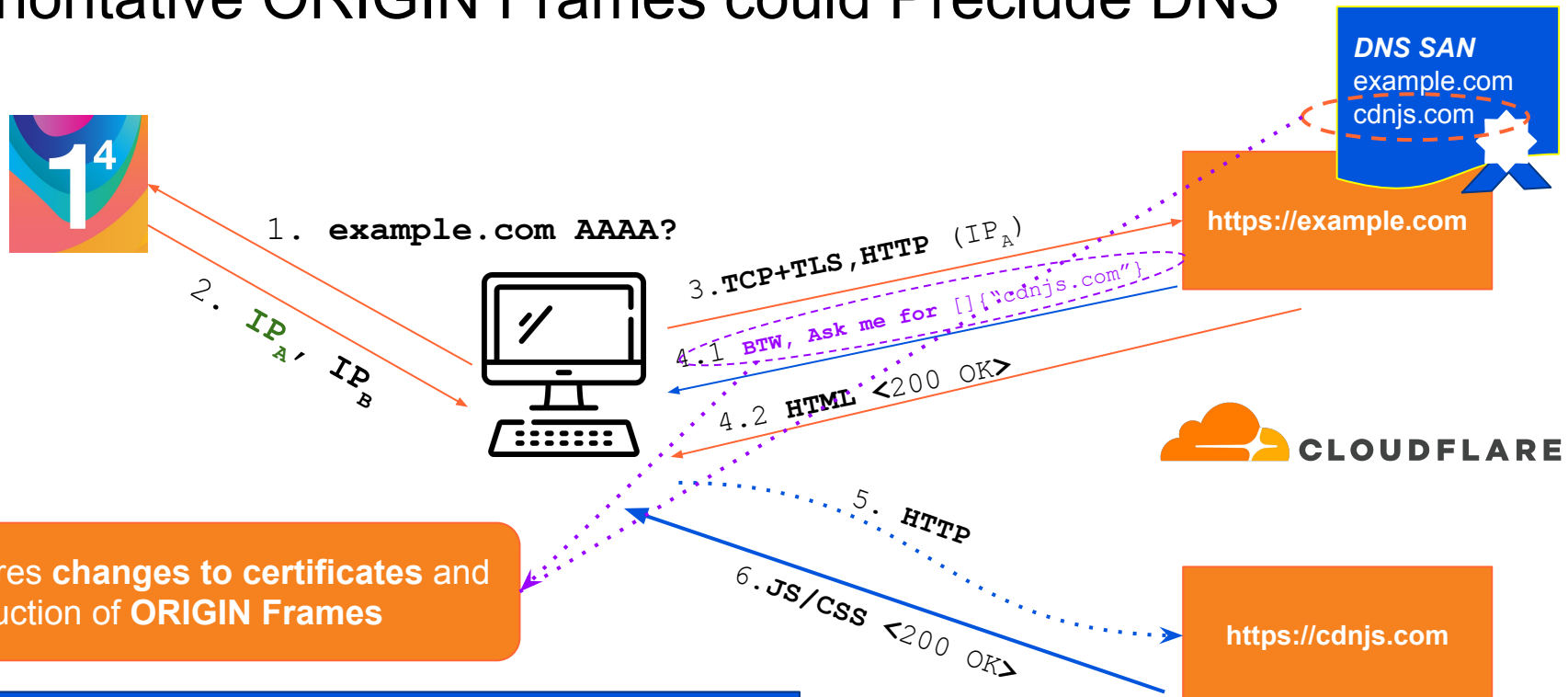
Most webpage resources are co-located on a few service providers despite being sharded by hostnames

Leveraging Colocation and Improving Privacy



Two separate TCP + TLS connections to two different IPs (IP_A, IP_B)

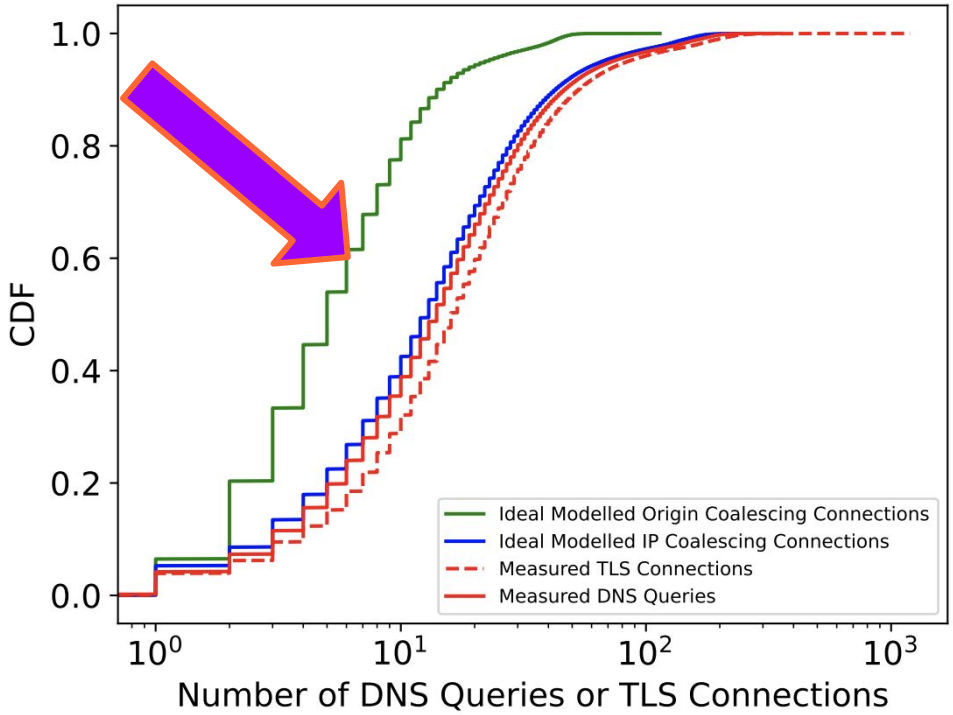
Authoritative ORIGIN Frames could Preclude DNS



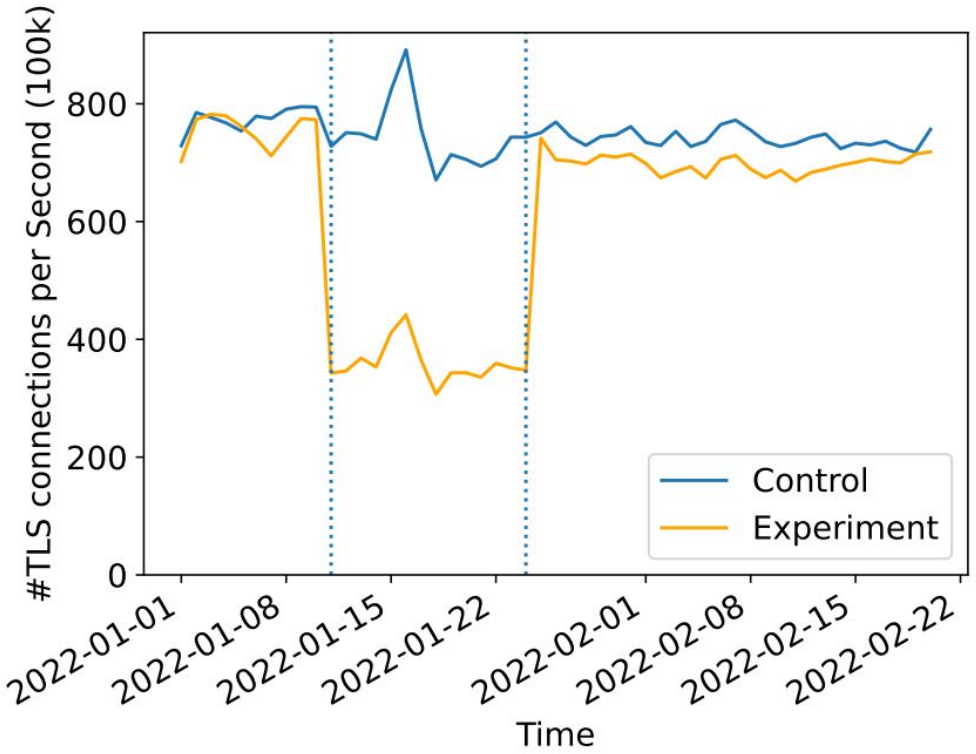
Requires **changes to certificates** and introduction of **ORIGIN Frames**

Could Prevent unwanted DNS queries if authority established

Over 60% Reduction in Number of DNS/TLS Connections



Deployment of ORIGIN Frames with Certificate Changes



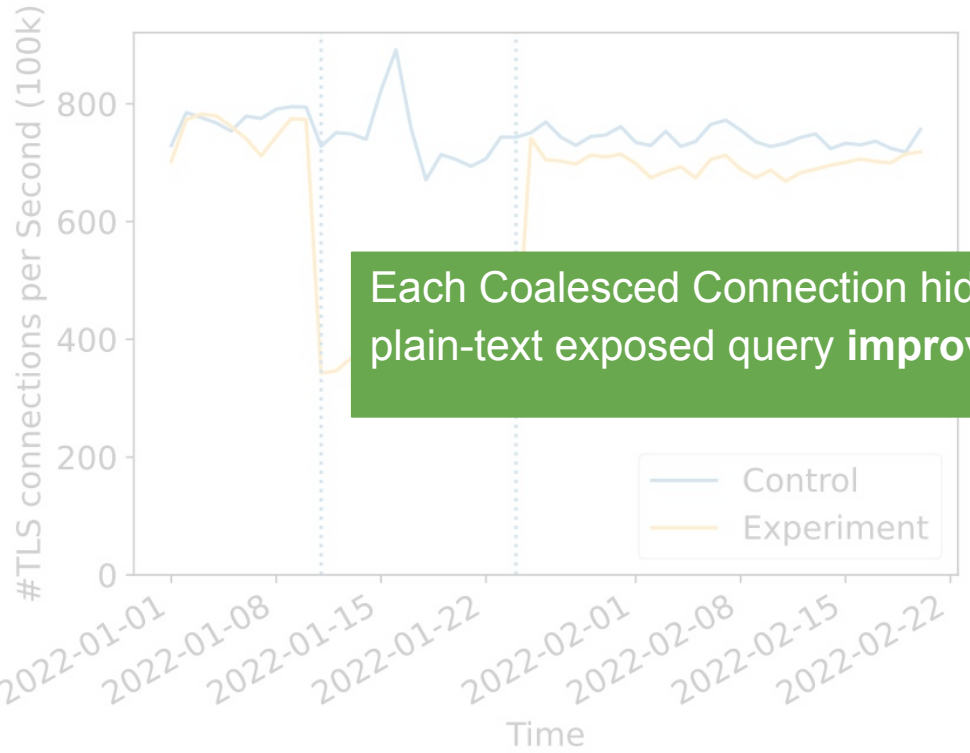
~50% reduction in number of new connections to the cdnjs hostname we attempted coalescing to.

Client: Reduced Number of Cryptographic Certificate Validations.

Client: Active measurements show ~65-70% connections coalesced.

Server: Reduced number of connections → allow more client connections

Deployment of ORIGIN Frames with Certificate Changes



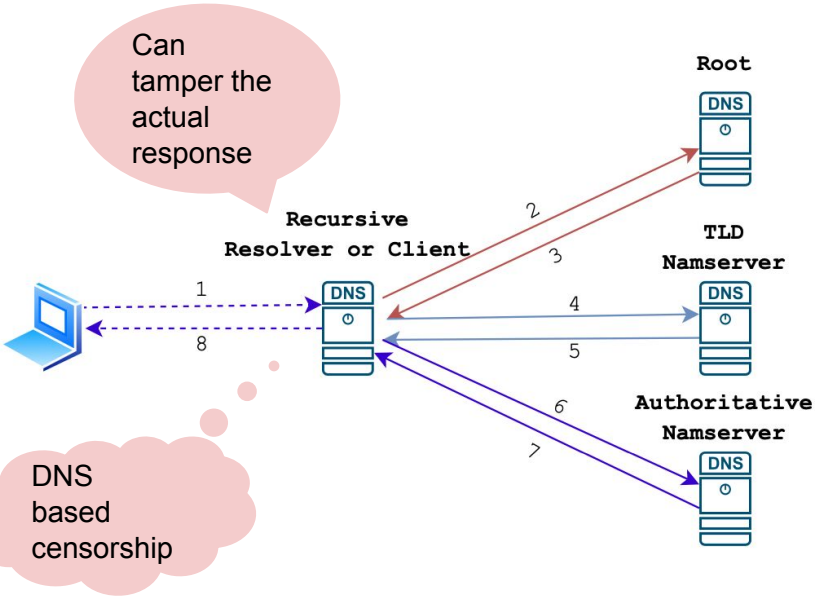
Each Coalesced Connection hides an otherwise plain-text exposed query **improving client privacy**.

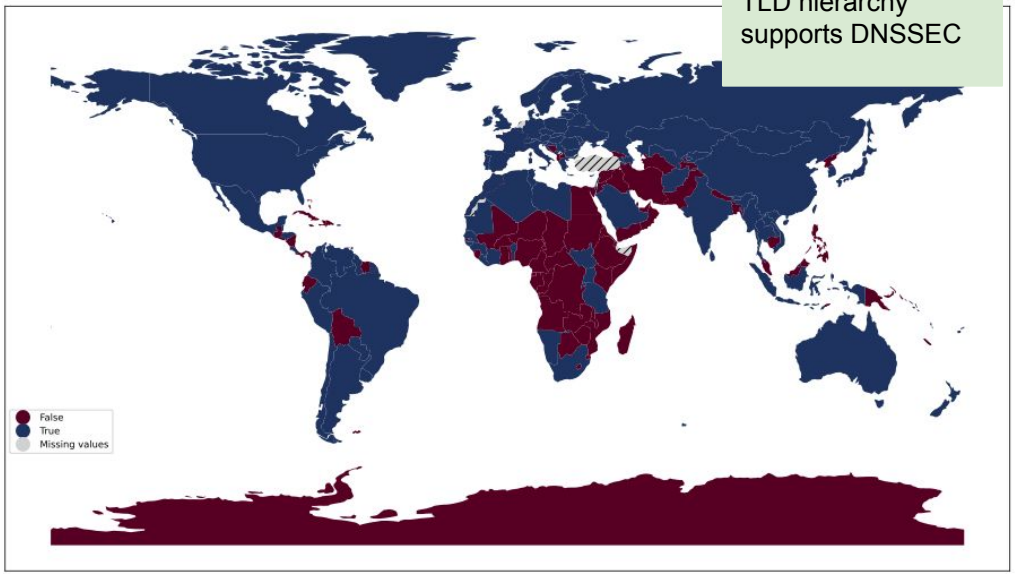
~50% reduction in number of new connections to the cdnjs hostname we attempted coalescing to.

Client: Active measurements show ~65-70% connections coalesced.

Server: Reduced number of connections → allow more client connections

Next Steps! Requesting Your Feedback





The benefits of DNSSEC cannot be provided until the TLD hierarchy supports DNSSEC

What **incentives** can we provide for improved DNSSEC adoption? How would that **impact** various DNS operations today? Is the **tradeoff worthwhile**?

Thank You!

Email: sudheesh@cs.washington.edu

https://sudheesh.info/

Graduating January - March 2024.

Open for exciting full time research and engineering opportunities. Please reach out!

Publications:

1. Singanamalla, Sudheesh, Suphanat Chunhapanya, Jonathan Hoyland, Marek Vavruša, Tanya Verma, Peter Wu, Marwan Fayed, Kurtis Heimerl, Nick Sullivan, and Christopher Wood. "**Oblivious DNS over HTTPS (ODoH): A Practical Privacy Enhancement to DNS.**" Proceedings on **Privacy Enhancing Technologies** 4 (2021): 575-592.
2. Singanamalla, Sudheesh, Muhammad Talha Paracha, Suleman Ahmad, Jonathan Hoyland, Luke Valenta, Yevgen Safronov, Peter Wu et al. "**Respect the ORIGIN! a best-case evaluation of connection coalescing in the wild.**" In Proceedings of the 22nd **ACM Internet Measurement Conference**, pp. 664-678. 2022.