Encryption without Centralization: Distributing DNS Queries Across Recursive Resolvers

Austin Hounsel, Paul Schmitt, Kevin Borgolte*, Nick Feamster†

Princeton University, Ruhr-University Bochum*, University of Chicago†

Contributions

- We present the design and prototype implementation of a **refactored stub resolver architecture that allows for de-centralized encrypted DNS resolution**

- We perform a preliminary evaluation of the stub resolver's performance

- We also utilize a real-world dataset to evaluate how query distribution strategies affect the queries seen by recursive resolvers

DNS Privacy Has Become a Significant Concern

- On-path network observers can infer website you are visiting
  - Governments, coffee shops, etc.

- Two protocols have been proposed to encrypt DNS traffic
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)

FIREFOX

Twitter

Firefox continues push to bring DNS over HTTPS by default for US users

Selena Deckelmann | **February 25, 2020**

Today, Firefox began the rollout of encrypted DNS over HTTPS (DoH) by default for US-based users. The rollout will continue over the next few weeks to confirm no major issues are discovered as this new protocol is enabled for Firefox's US-based users.

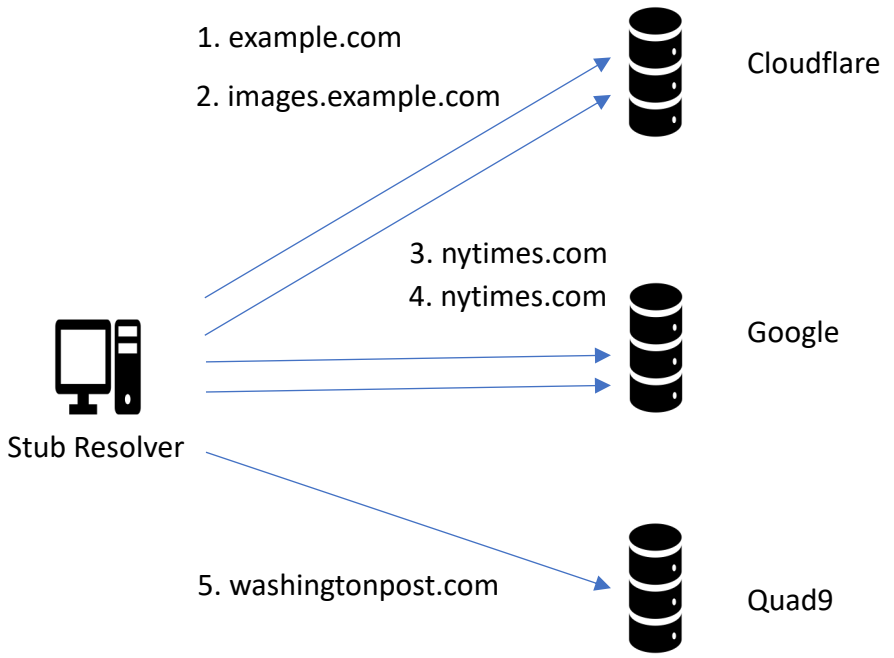
Research Questions

1. Is de-centralization worth doing?

2. **This paper: If so, how could it be technically possible/feasible? What forms could decentralization take?**
   If it's not technically feasible, then it's not even worth debating about whether it's worth doing!

Re-Decentralizing Encrypted DNS: Technical Architecture

1. The stub resolver discovers resolvers that support DoH, along with characteristics of those resolvers (e.g., geographic location)
2. The user articulates requirements (e.g., a preference to avoid a specific location or ISP)
3. The stub selects a **set** of DoH resolvers by matching characteristics with preferences
4. The stub **distributes queries across multiple DoH resolvers** according to some user-specified strategy

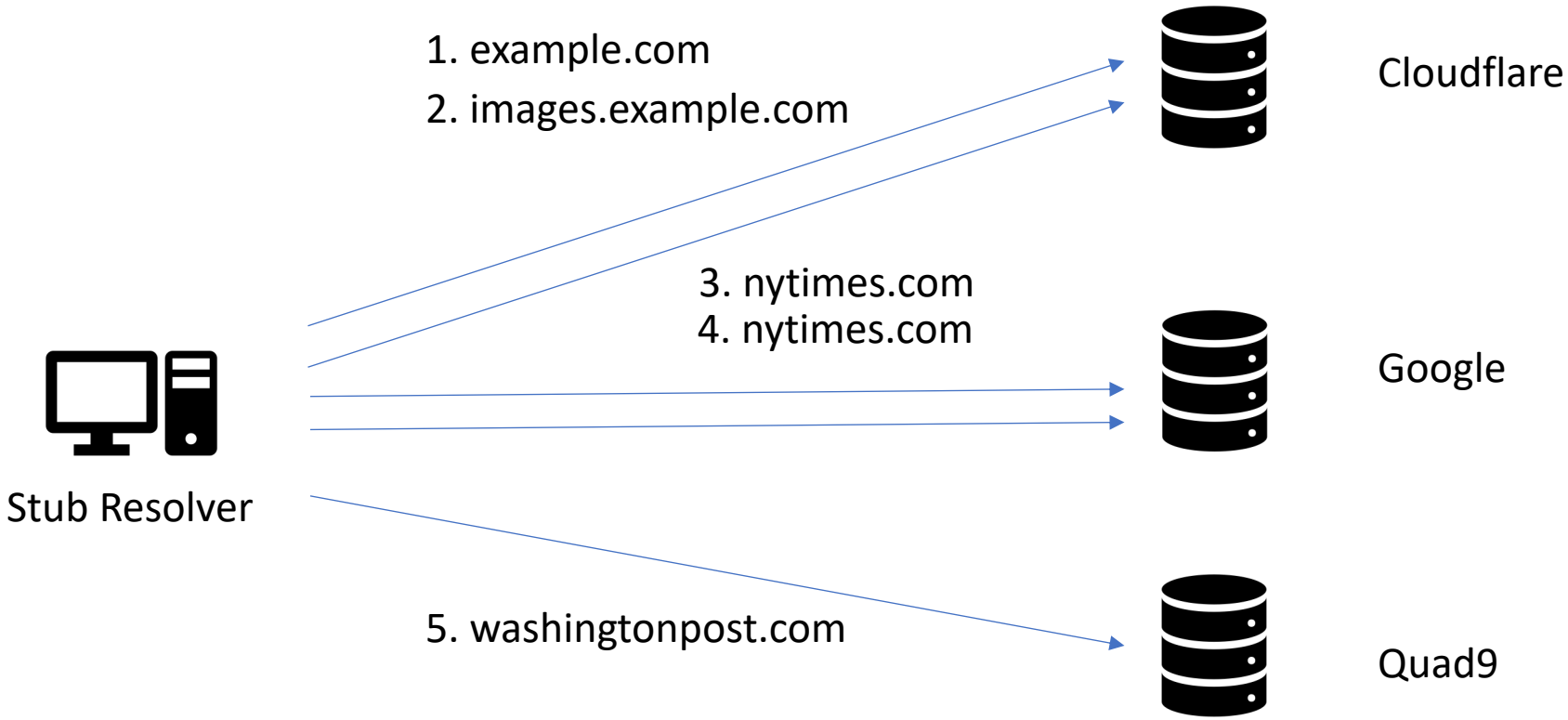


Prototype Implementation

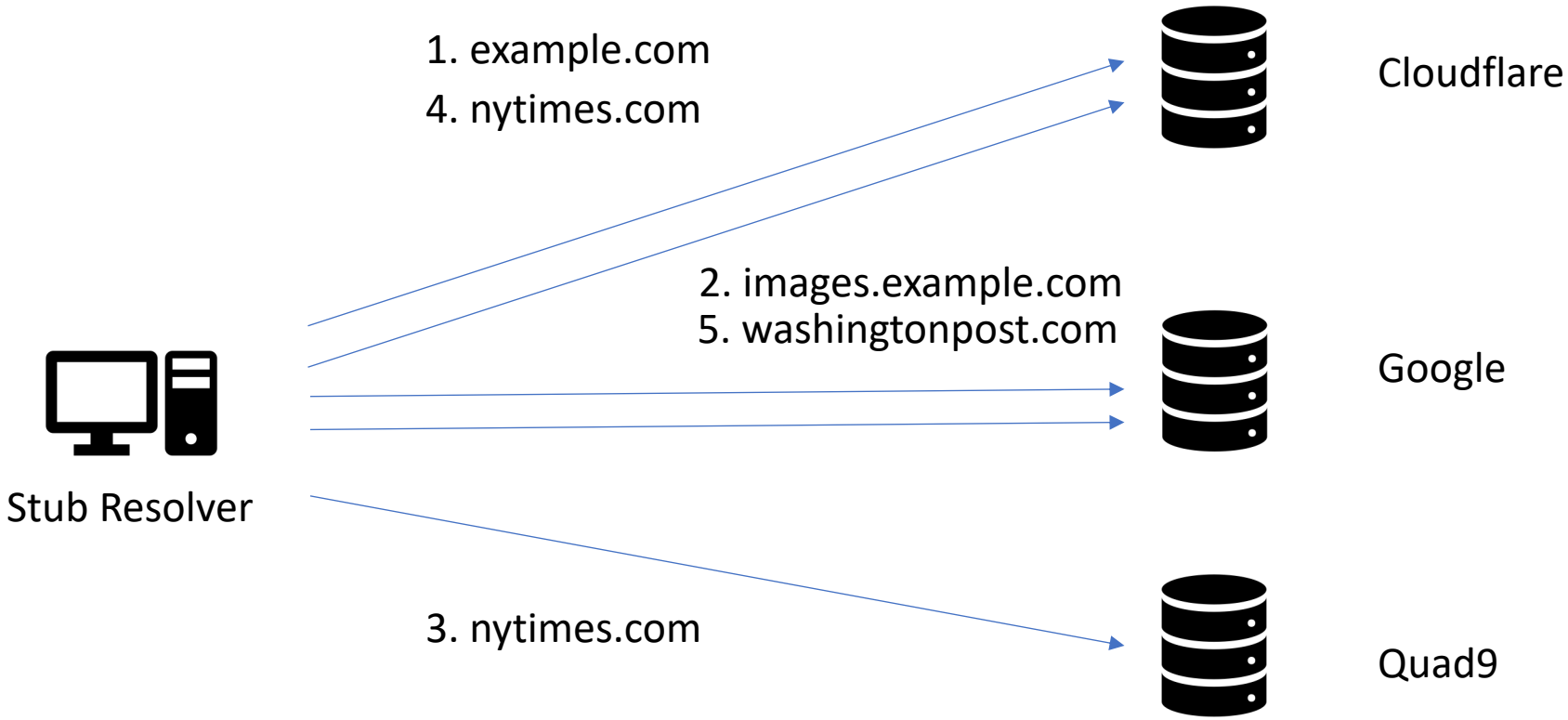
- Fork of open-source encrypted DNS proxy dnscrypt-proxy [1]
- Supports hash, round-robin, and random query distribution
- Can run on host devices and routers

[1] https://github.com/noise-lab/ddns

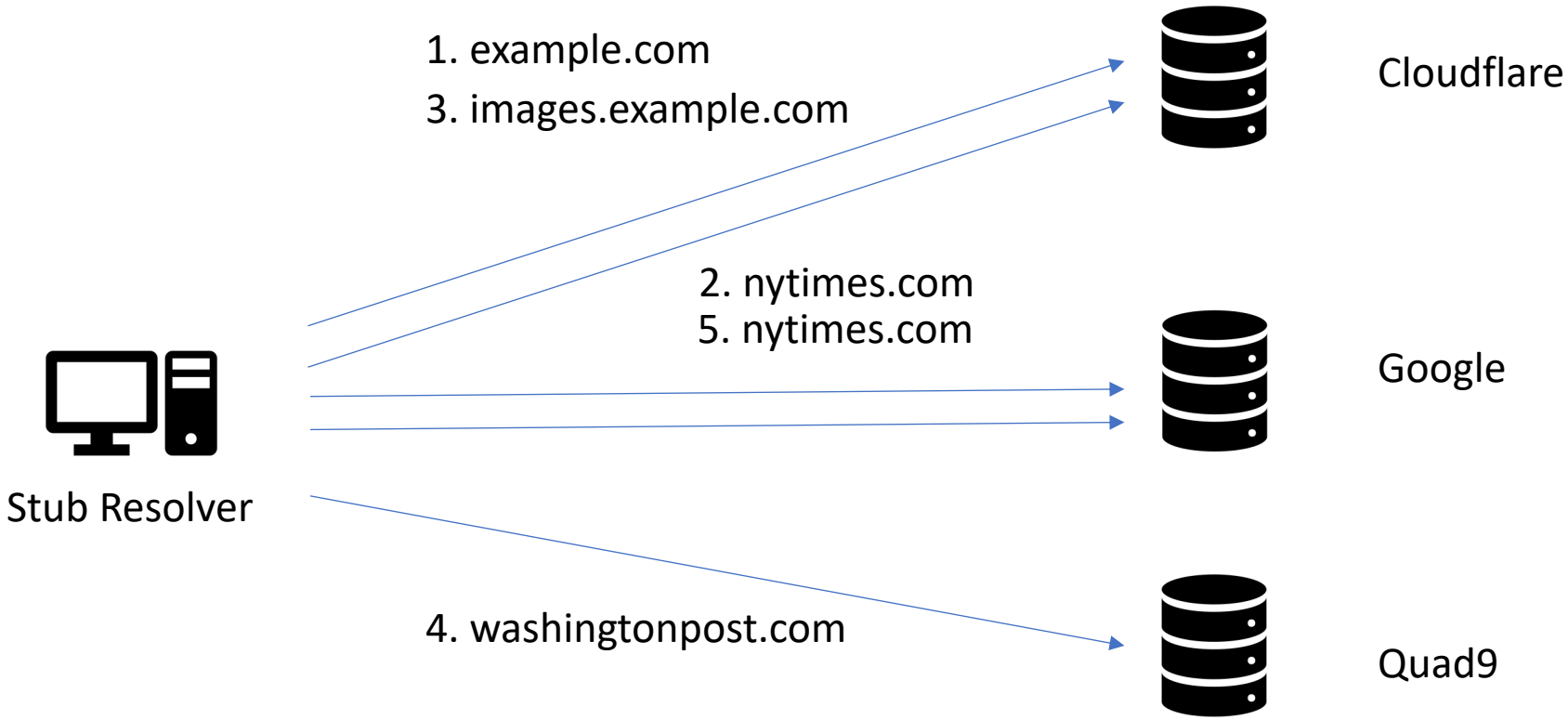
Query Distribution: Hashing



Query Distribution: Round-Robin



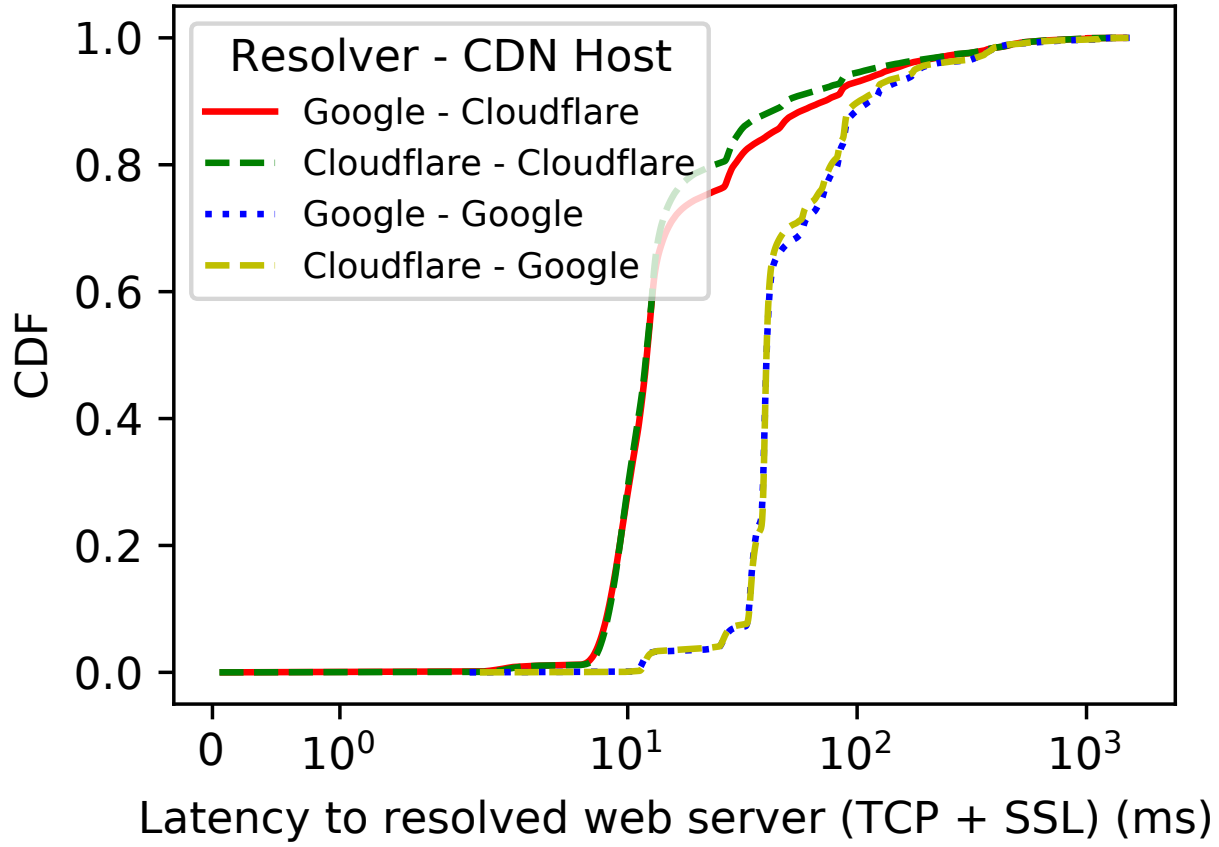
Query Distribution: Random



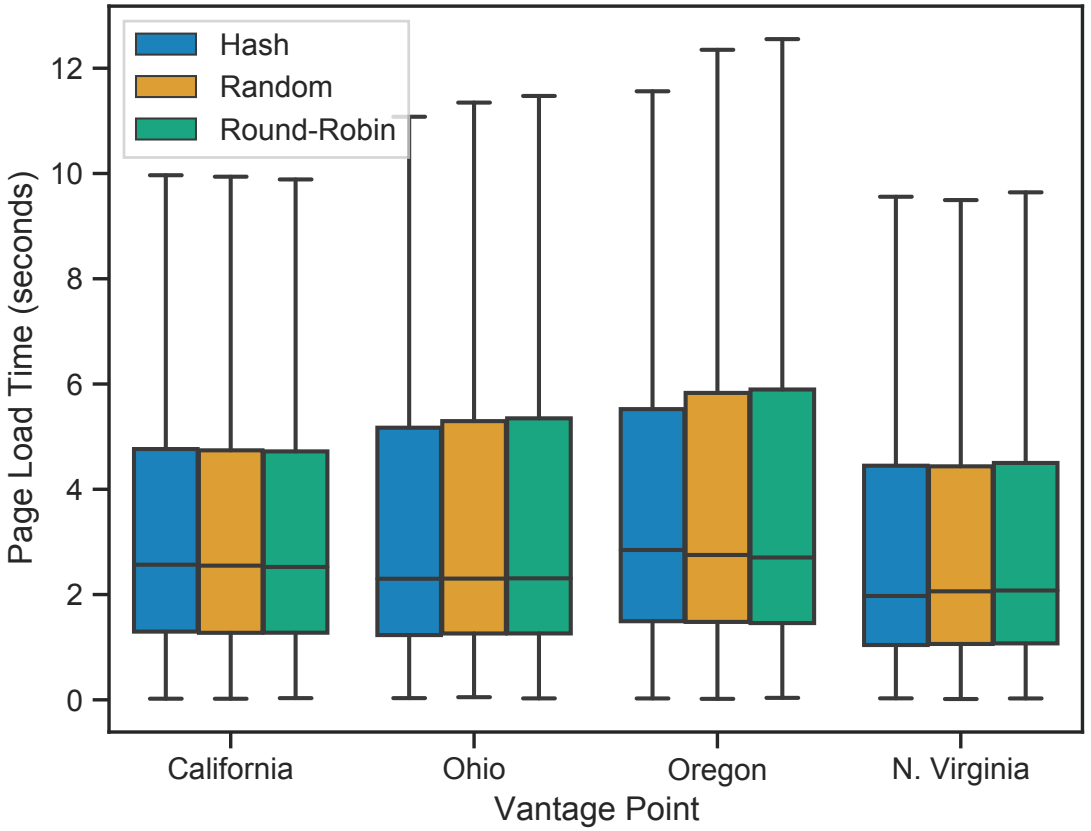
Evaluation Questions

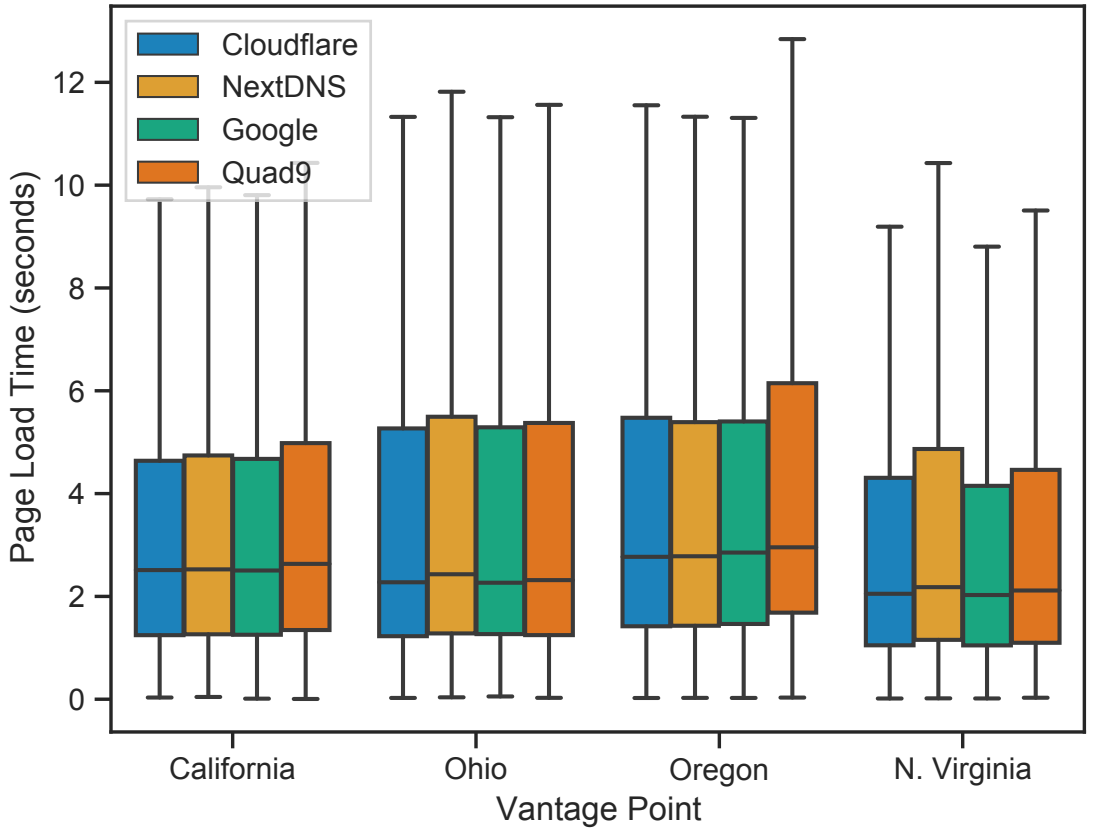
- Performance
  - CDN localization
  - Page load times
- Privacy
  - # of domain names seen by resolvers

Effect on CDN Localization

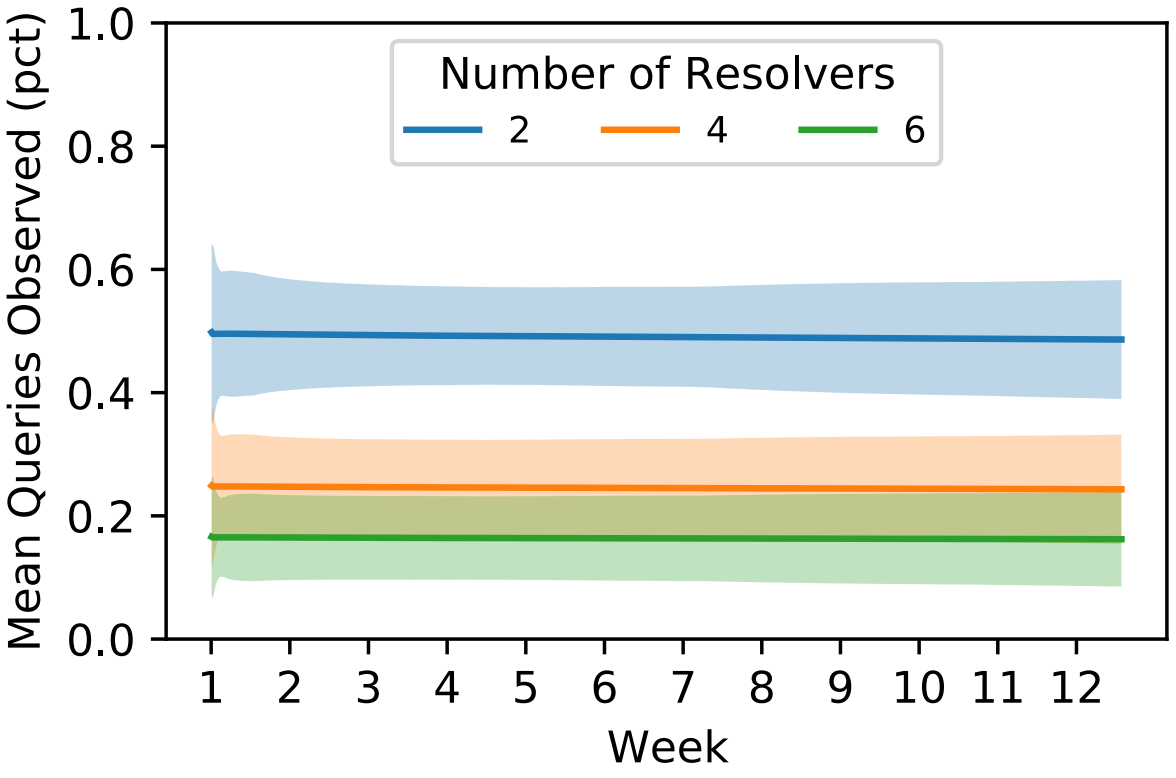


Effect on Page Load Times

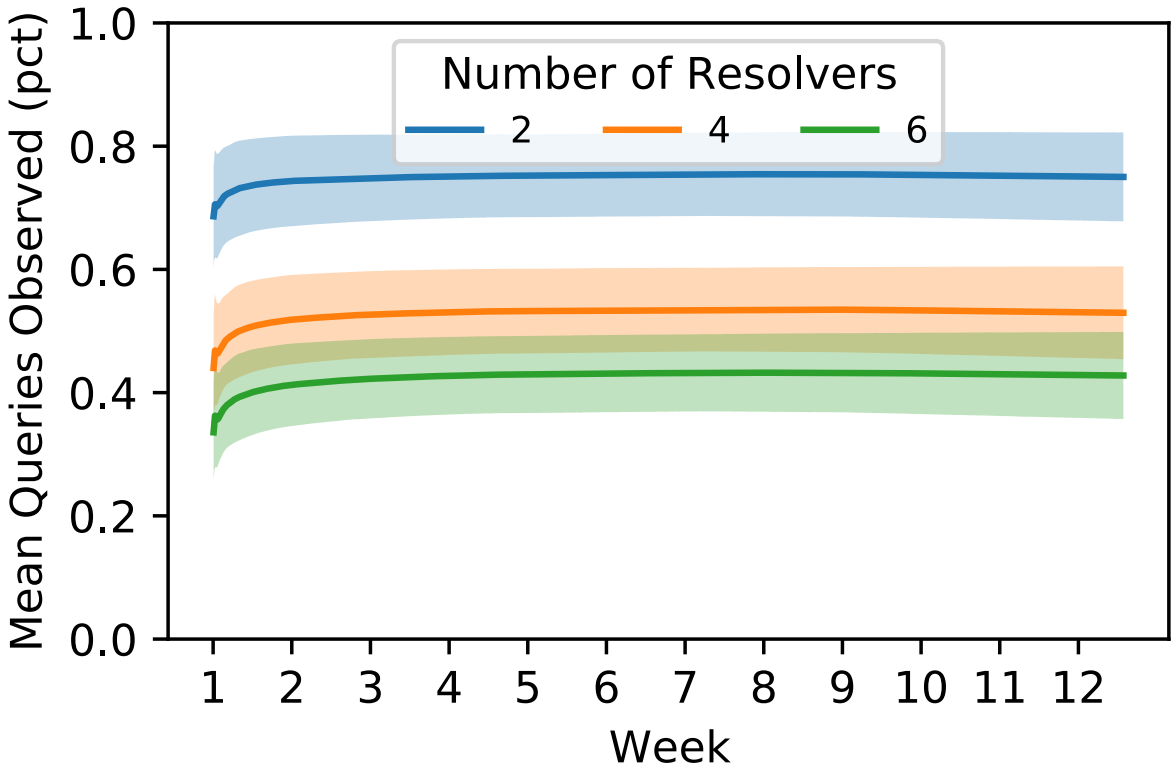




Effect on Domain Names Seen By Resolvers



(a) Hash distribution on second-level domain names



(b) Round-robin distribution

Summary

- We present the design and prototype implementation of a **refactored stub resolver architecture that allows for de-centralized encrypted DNS resolution**

- We perform a preliminary evaluation of the stub resolver's performance

- We also utilize a real-world dataset to evaluate how query distribution strategies affect the volume of queries seen by recursive resolvers

Thank you!

Contact: Austin Hounsel

ahounsel@cs.princeton.edu