CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

VolkswagenStiftung

Web Privacy By Design: Evaluating Cross-layer Interactions of QUIC, DNS and H/3

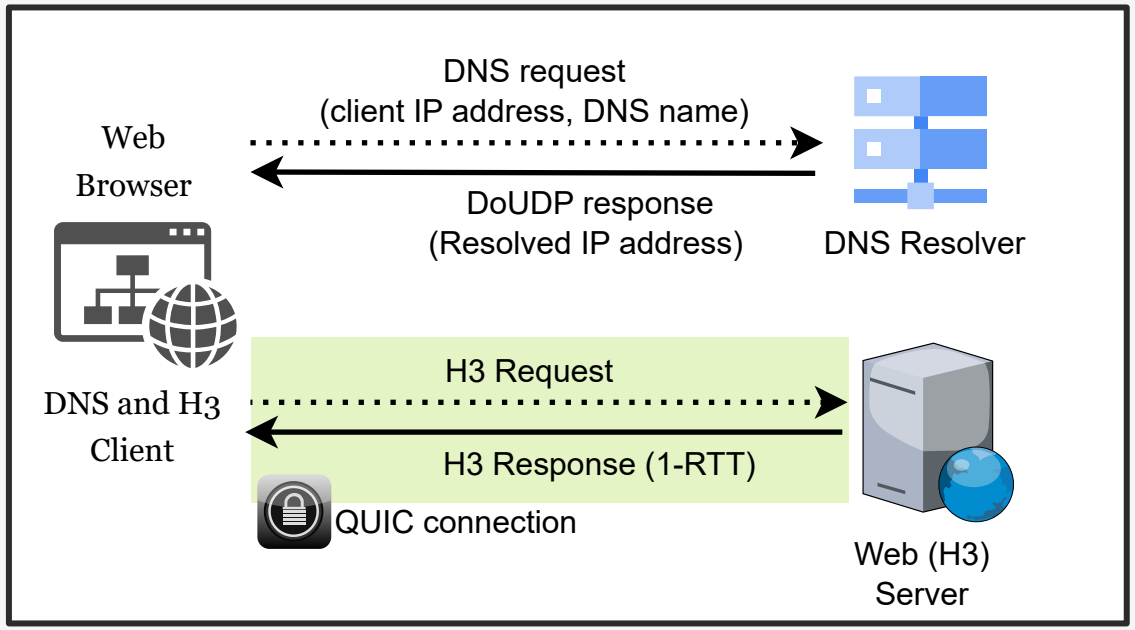
Jayasree Sengupta | CISPA Helmholtz Center for Information Security, DE
Mike Kosek, Justus Fries | Technical University of Munich, DE
Pratyush Dikshit, Vaibhav Bajpai | CISPA Helmholtz Center for Information Security, DE

Published at IFIP Networking Conference, June 2023

IETF 117, San Francisco
MAPRG (Remote) | 28 July 2023

Motivation

- Unencrypted DNS resolution using DNS over UDP (DoUDP)
- Browsers offer to encrypt DNS traffic using DNS over HTTPS (DoH)
- Both DoH and DoT are constrained by several factors
  - head-of-line blocking
  - multiple round-trips
- DNS over QUIC (DoQ) is the new player
  - benefits from faster handshakes
  - HTTP/3 (H3) avoids multiple handshakes
- Even using QUIC with DoQ and H3, improvements are uncoupled



Existing mechanism of Web browsing

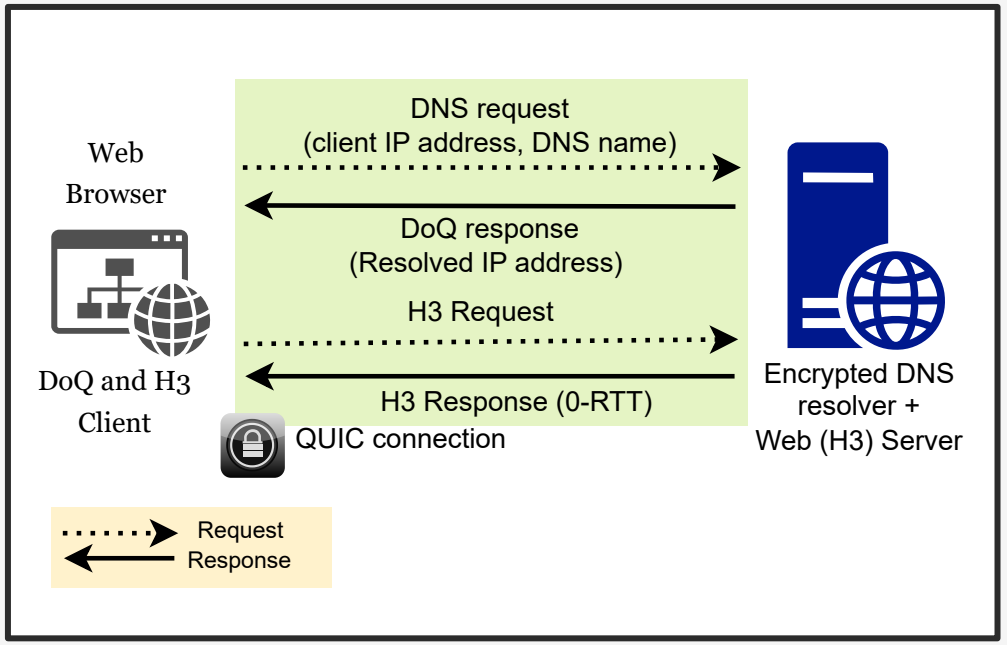
How to improve Web browsing experience with inbuilt *Web Privacy by Design*?

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Motivation and Research Question

- Utilise the same underlying QUIC connection for:
  - DNS resolution using DoQ
  - Web content delivery using H3 with 0-RTT
  - Also, fresh H3 request to the Web server

- Offers optimisation potential
- Web communication becomes private and faster



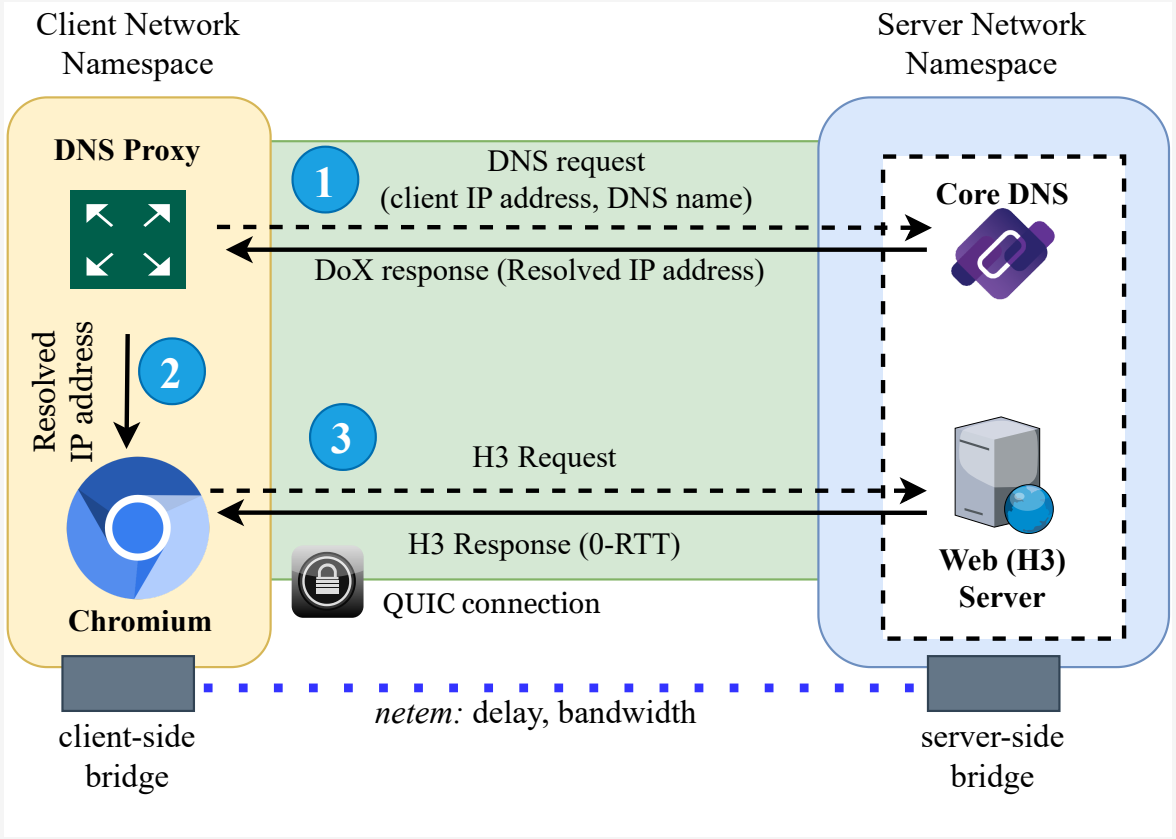
Proposed mechanism of Web browsing

What is the impact of reusing the same QUIC connection on Web Performance?

How it impacts over both fixed and mobile access network technologies?

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Methodology



Measurement setup to evaluate DoQ + H3 0–RTT

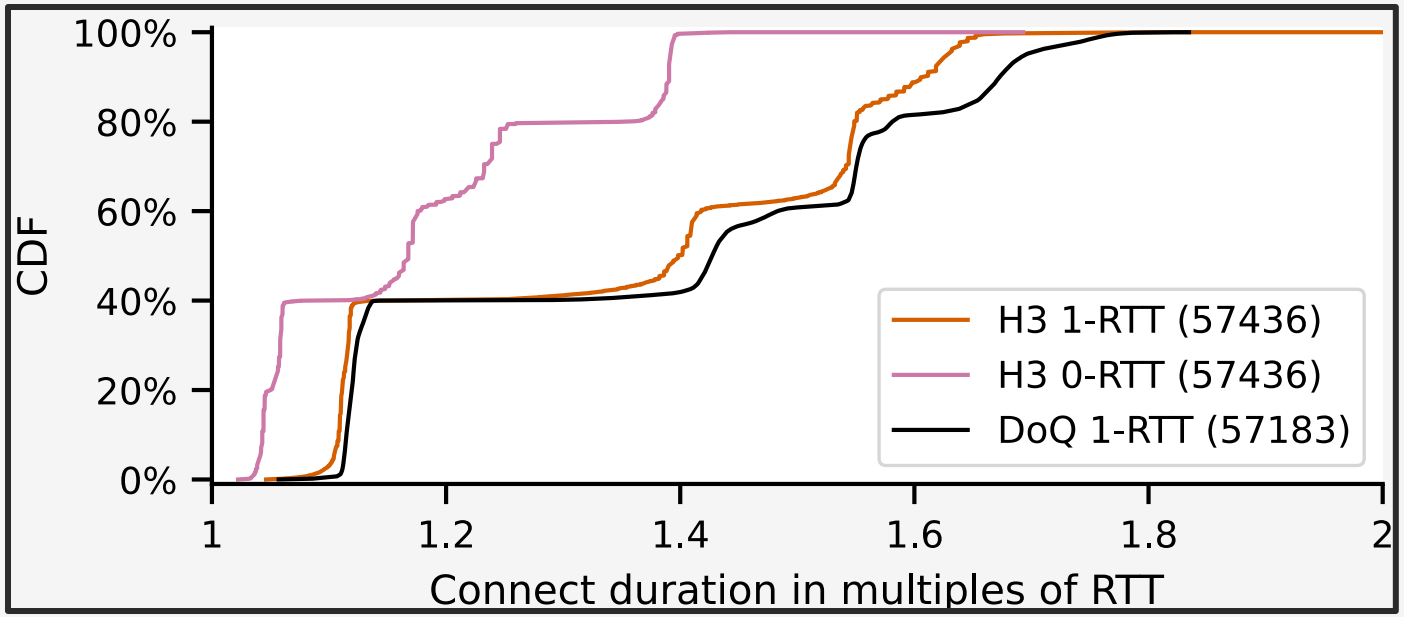
- Categories of web pages measured with their sample sizes:
  - an HTML page (example.org): 114,924
  - an HTML page with javascript assets (wikipedia.org): 114,882
  - an HTML page with javascript assets, CSS and cookies (instagram.com): 114,810
- Different network conditions are simulated using *netem*:
  - Fiber (68,934), cable (68,916), DSL (68,928), 4G (68,922) and 4G medium (68,916)
  - FCC's Measuring Broadband America dataset represents fixed broadband scenarios
  - ERRANT dataset represents mobile wireless access technologies

- *CoreDNS* is extended to run an H3 server in order to share TLS information
- *Chromium* is modified to support importing and exporting TLS session information
- Data points are normalised by the scenario's delay or round-trip times for the access technologies

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: QUIC Handshake Connect Duration

How QUIC interacts with DoQ and H3?



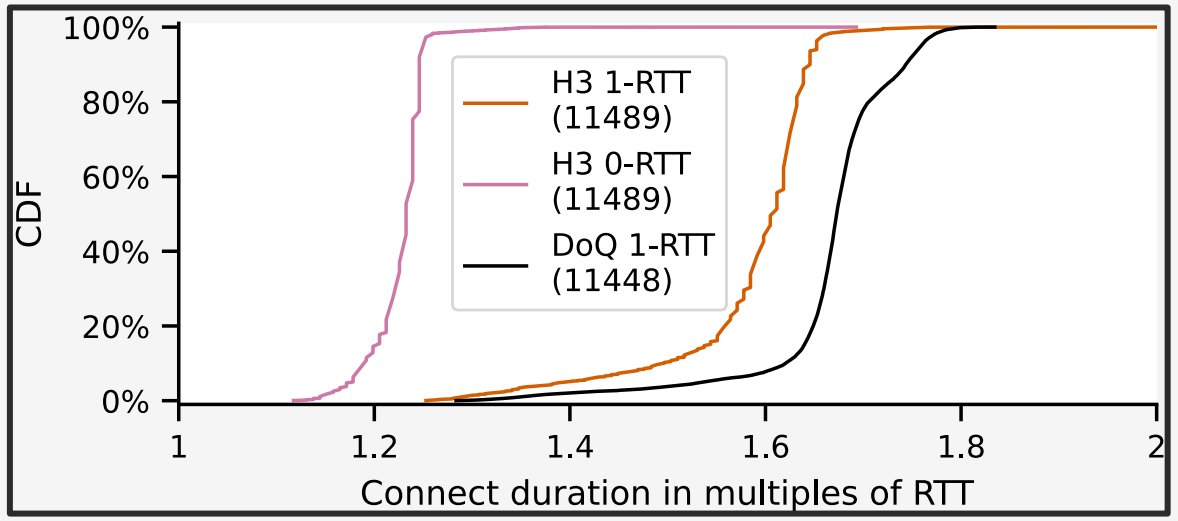
- H3 1-RTT connect times roughly corresponds to DoQ handshake times
- Difference between H3 0-RTT and H3 1-RTT is less than one round- trip
- Distinct step pattern caused by differences in access technologies

Performance of DoQ and H3 1-RTT are majorly synchronised. In general, metrics scale with round-trips showing distinct steps for different access technologies.

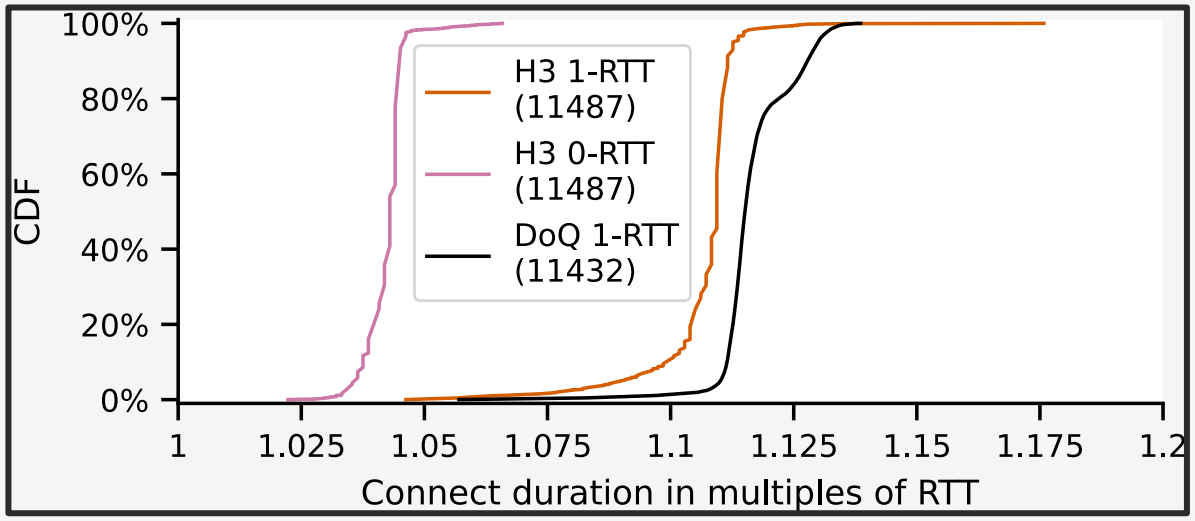
Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: QUIC Handshake Connect Duration

What is QUIC's scaling capability while interacting with DoQ and H3 under different network conditions?



Fibre Scenario



4G Scenario

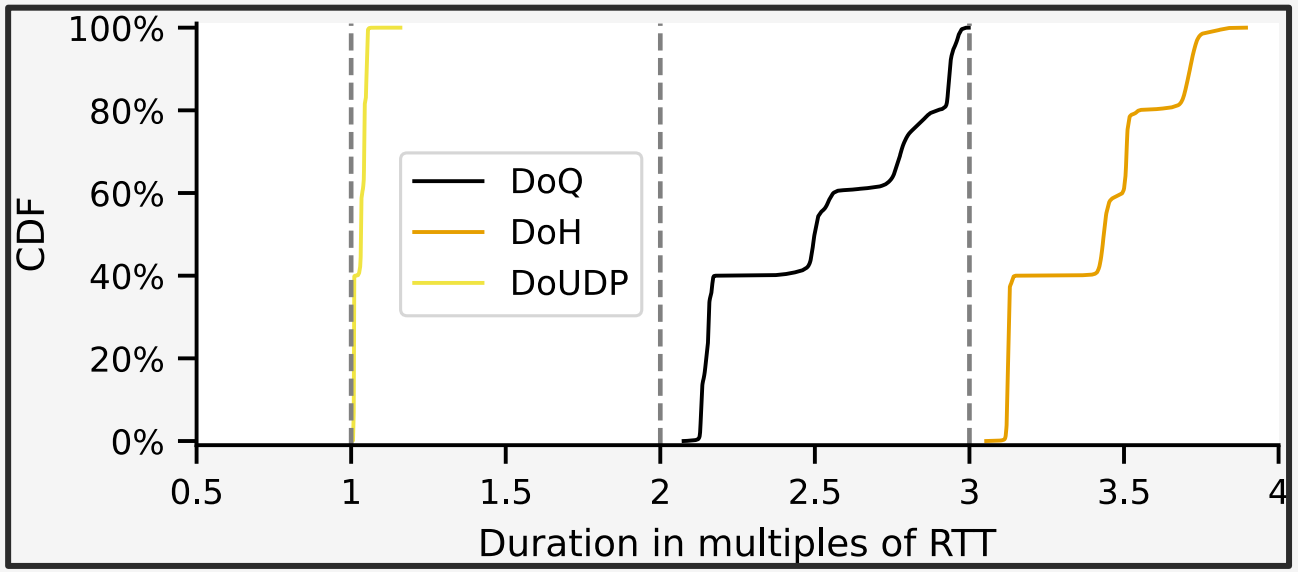
- *connect times* have a long tail in the high percentiles
- 1-RTT has a relatively large left tail from minimum to the 20th percentile
- Actual data for 0-RTT has less variation compared to 1-RTT
- 4G handshake time scales better with RTT while having less variation

Processing delay is large for lower RTT access technologies. While, in absolute terms, processing delay is same for high RTT access technologies, it weighs in much less relatively, resulting in the observed differences being small between H3 0-RTT and 1-RTT. However, 0-RTT still shows *connect* times.

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: DNS Exchange Duration

What is the overhead of DoQ and DoH in comparison to DoUDP?



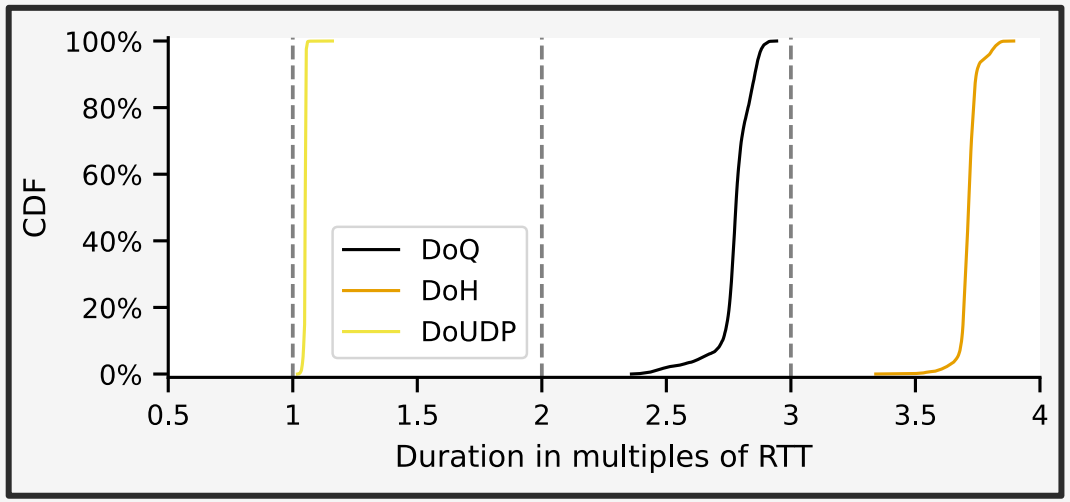
- Steps are visible for DoQ and DoH, but not for DoUDP
- Five steps in 20 percentile intervals are seen which represents different access technologies
- DoQ and DoH do not appear to exhibit the expected number of round-trips

DoQ and DoH do not exhibit the expected number of round-trips, only DoUDP does. DNS exchange duration of DoQ is one round-trip faster than DoH.

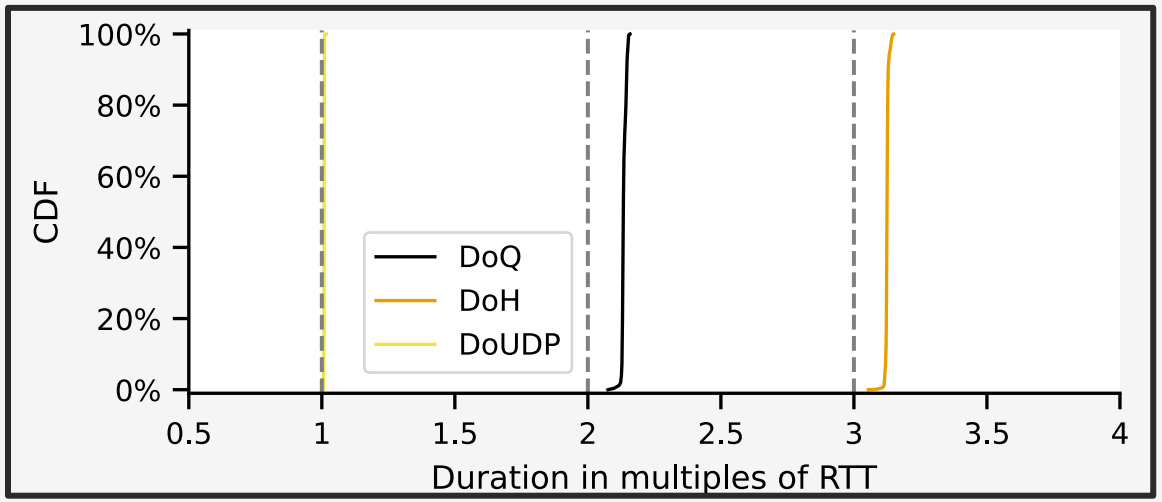
Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: DNS Exchange Duration

How does the DNS protocols scale over different network conditions?



Fibre Scenario



4G Scenario

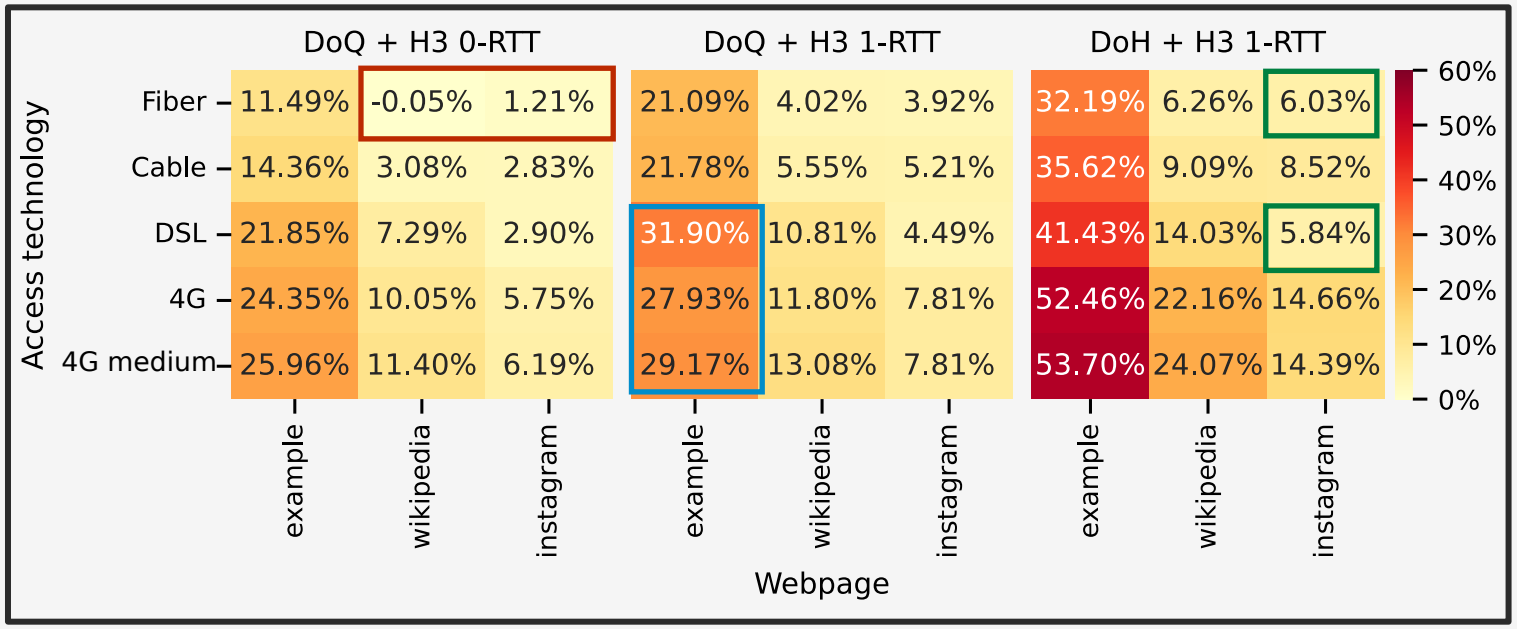
- Left tail for lower percentiles is visible for both DoQ and DoH
- Left tail appears to be the largest for fiber and eventually gets smaller for 4G
- Range of values for 4G is much smaller implying less variation in the data

Lower RTT access technologies exhibit longer left tails, which eventually get smaller with increasing delay.

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: Overall Impact of DoQ + H3 0-RTT

What is the performance of the emulated DoQ + H3 0-RTT setup across different access technologies and webpages compared to its competitors?



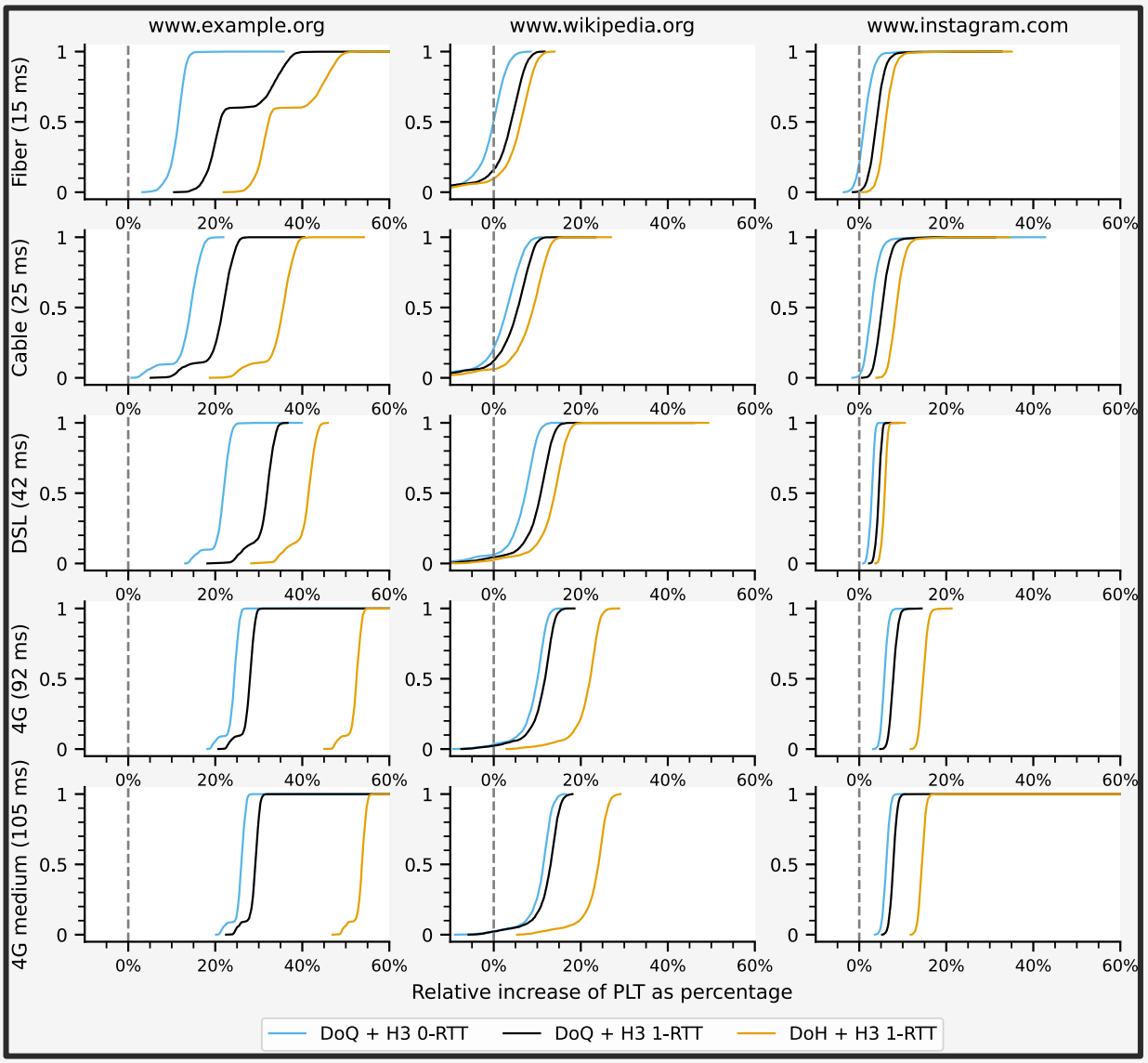
Relative median PLT increase over DoUDP baseline

The emulated DoQ + H3 0-RTT performs best across all webpage and access technology combination. Moreover, it replicates performance similar to the baseline when replaying the *wikipedia page* over fiber.

- DoH has the highest relative increase across all web pages and access technologies
- The *example page* shows the highest relative increase
- Relative increase for the *wikipedia page* is greater than *instagram page*
- Performance of the access technologies degrade in an order of the respective round-trip delay

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: Overall Impact of DoQ + H3 0-RTT

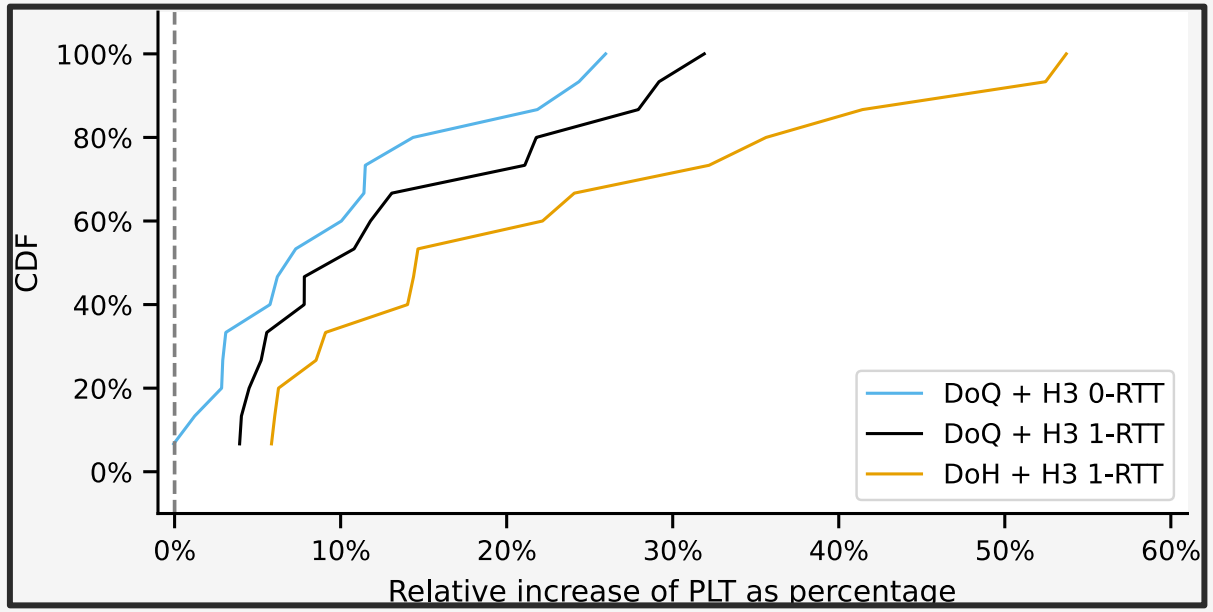


- For all access technologies:
  - *example page* has a short left tail, except for fibre
  - *wikipedia page* has a longer left tail
  - *instagram page* has no tail
- Differences in percentage points between the protocol combinations
  - Largest: *Wikipedia*
  - Smallest: *Instagram*
- Difference between DoQ and DoH:
  - scales with the round-trip time, except for DSL
- Difference between H3 0–RTT and 1–RTT:
  - does not scale with round-trip time as expected
- But, percentage point difference between DoQ and DoH increases with increasing RTT

Both dimensions have an effect on the relative increase over the baseline. Increasing delay between client and server, reduces potential time savings of 0-RTT, while savings for using DoQ instead of DoH increases.

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Evaluation: Overall Impact of DoQ + H3 0-RTT



Median Relative increase across protocol combinations over DoUDP baseline

Using H3 1-RTT, PLT for DoH is inflated by >30% over fixed-line and by >50% over mobile compared to unencrypted DoUDP. However, DoQ+ H3 0-RTT reduces PLT by 1/3 over fixed-line and 1/2 over mobile compared to the existing setup.

- Each protocol combination has 15 data points, one for each *[web page, access technology]* tuple
- DoQ + H3 0-RTT setup matches the baseline for one tuple (median relative increase is 7.3%)
- Median of DoQ setup is slightly higher at 10.8%
- DoH setup has an average relative increase of 14.7%
- Even in the worst case scenario:
  - DoQ + H3 0-RTT is at 26.0%
  - DoQ is at 31.9% and DoH is at 53.7%

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Limitations and Future Work

Limitations:

- Presented findings represent an emulated setup, DNS name resolution has been decoupled from the web browsing process
- Measurement setup of QUIC connection coalescing using DOQ + H3 for 0–RTT is currently
  - limited to web pages having a single DNS resolution
  - implemented with a single H3 Web server which is an uncommon scenario
- For websites with several DNS resolutions, a scaling factor needs to be applied to the results presented here

Future Work: Refine the introduced concept of QUIC connection coalescing by extending:

- Chromium with support for DoQ in order to couple DNS resolution with Web browsing
- The methodology to:
  - Web pages with more than one DNS resolution
  - emulate packet loss and cross-traffic network conditions
- DoH3 support for blurring the boundaries between DNS resolution and Web content delivery

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security

Takeaway

- DoQ + H3 0-RTT performs best across all webpage and access technology combination
- Even in the worst case scenario, DoQ + H3 0-RTT performs the best
- DoQ with H3 0-RTT reduces page load times by:
  - 1/3 over fixed- line
  - 1/2 over mobile

compared to existing Web browsing scenario, taking Web Privacy By Design to the next level

Paper

bit.ly/3MWleMS

Code

bit.ly/45S1bHQ

DoQ + H3 0-RTT is the best option for encrypted communication on the Internet

Jayasree Sengupta | jayasree.sengupta@cispa.de | CISPA Helmholtz Center for Information Security