Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

11th October 2018
PET-CON 2018.2

User Tracking via Google's QUIC Protocol

Erik Sy, M.Sc.

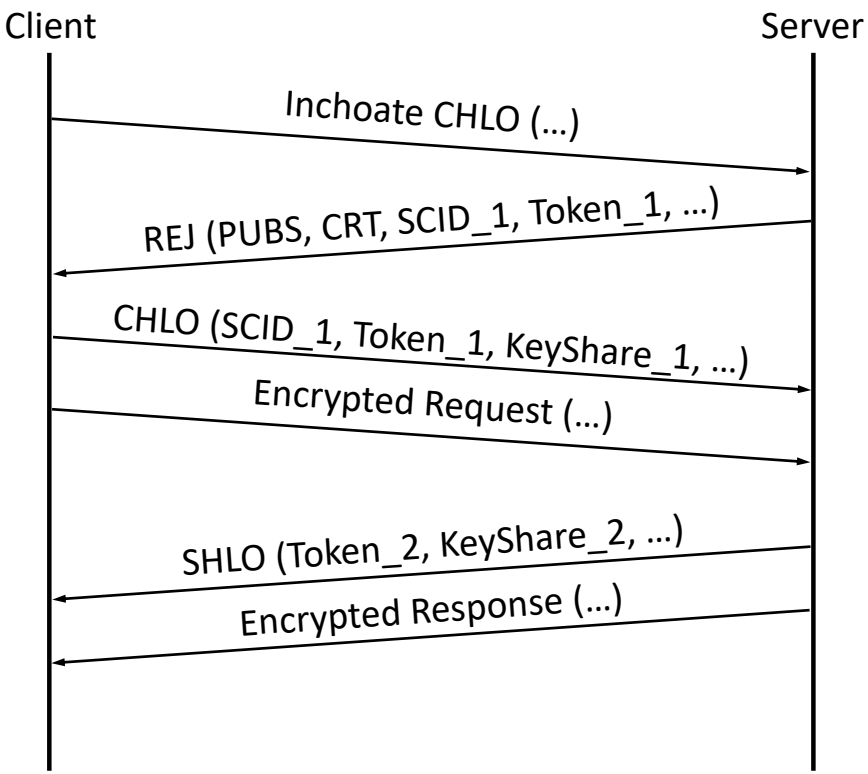
Introduction to the QUIC Transport Protocol

- QUIC over UDP provides an alternative HTTPS stack to TLS over TCP
  - Allows for zero round-trip time secure connection establishment

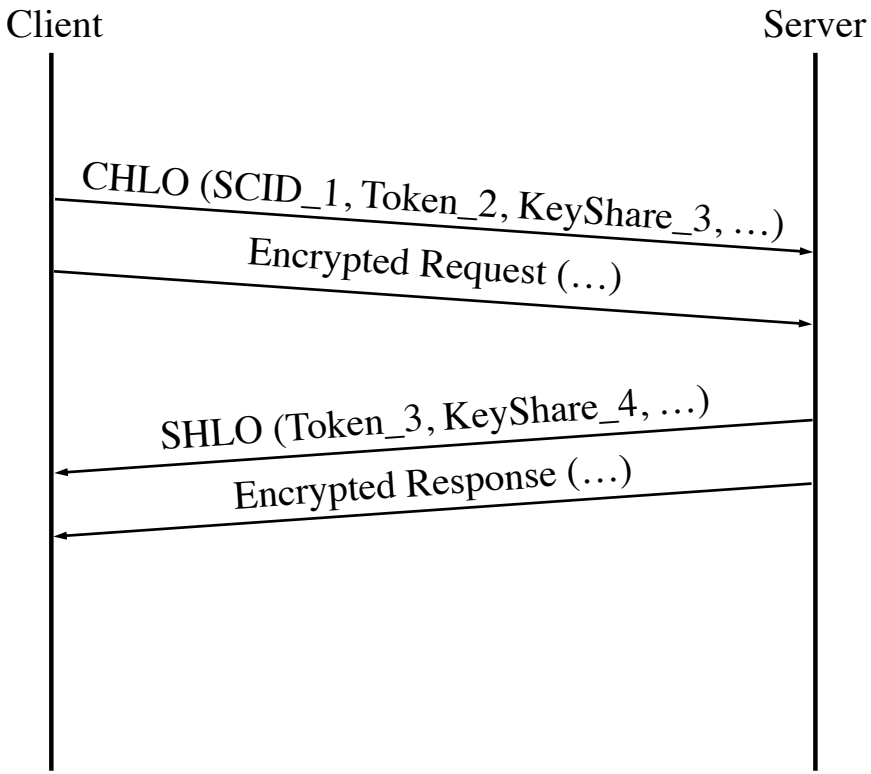
- Deployment on the Internet
  - accounts for 7% of global Internet traffic
  - more than five million hosts in IPv4 currently support QUIC
  - supported by Google Chrome (approx. 60% browser market share)
  - other use cases include DNS over QUIC, FTP over QUIC, SMTP over QUIC

QUIC's Connection Establishment

- QUIC reuses cached *server config* and *token* across several user sessions



a) Initial Handshake



b) Subsequent Handshake

Opportunities and Limitations of Tracking via QUIC

- Independent of common tracking approaches like IP addresses, HTTP cookies and browser fingerprinting

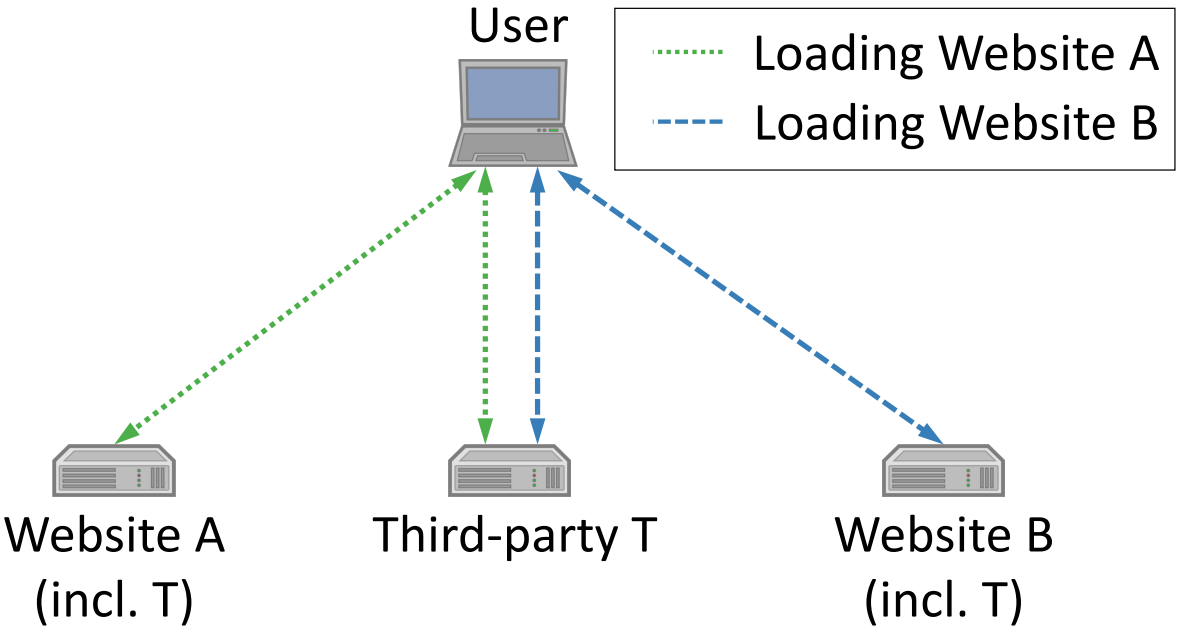
- Opportunities compared to browser fingerprinting
  - Faster unique identification of a user
  - Lower consumption of bandwidth and computational resources

- Limitations
  - Browser restarts terminate a tracking period
  - QUIC configuration of a browser
    - Lifetime of *Token* and *server configs*
    - Feasibility of third-party tracking

Experiments to test Browsers' default QUIC Configuration

- Measurement of QUIC's Token lifetime within popular browsers
  - Maximum delay between two website visits for which the browser still attempts to establish the new connection with an cached Token

- Investigating the feasibility of third-party tracking via QUIC



Summary on the Browser's default QUIC Configuration

Browser	**Lower boundary of Token's lifetime**	**Third-party Tracking**
Chrome	20 days	viable
Opera	18 days	viable
Chromium	20 days	viable
Chrome (mobile)	11 days	viable

Countermeasures

- Browser vendors must align tracking via QUIC with HTTP cookie policies
  - Disabling third-party tracking via QUIC through sandboxing
  - Limiting the lifetime of cached QUIC data to a single page visit if not cookies are set by that website
  - Prevent a reset of the Token's and server config's lifetime
- Connection establishments based on public key cryptography require mechanisms to assure that public keys are not unique per user
- Privacy advocates
  - Observed browser behaviour seems not to comply with principles of privacy by design and privacy by default (Article 25 of GDPR)

Conclusion

- Zero round-trip time secure connection establishment requires prefetched data which can be potentially abused for tracking
- Tracking via QUIC is a real-world privacy problem which allows the tracker to circumvent strict HTTP cookie policies and IP address changes
- Countermeasures require the action of browser vendors

Thank you

Questions and Answers

E-mail: sy@informatik.uni-hamburg.de

Preprint: Please request pre-print article per email.