

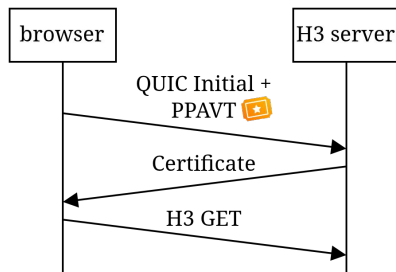
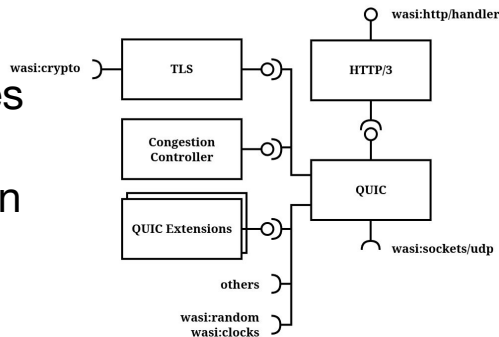
Benedikt Spies

PhD Student @ Chair of Connected Mobility @ TUM



Research Interest:

- Performance Enhancing Proxies
- Connection and State Migration
- Middlebox Discovery
- Web Performance and Security



- Is web tracking a lost game? Is it worth tackling tracking vectors on the transport layer?

Chair of Connected Mobility
School of Computation, Information and Technology
Technical University of Munich

TUM

Third-Party Tokens for QUIC Address Validation

Benedikt Spies, Nico Greger, Jonathan Kaleve, and Justus Fries

QUIC

QUIC [RFC 9000] enables fast connection establishment for HTTP/3 in RTT.

To prevent amplification attacks a QUIC server must limit the amount of data sent to an unauthenticated address to 3x the amount of data received from the client.

The client address is validated after 1 RTT or with an Address Validation Token (AVT).

- QUIC trades performance for privacy [1]
- Large certificates probing handshakes [2]

QUIC Handshake

Many QUIC handshakes cannot be completed within 1 RTT because the response of the server exceeds the anti-amplification limit.

Address Validation Token (AVT)

AVTs are shared by the QUIC server in **NEVER** / **COOKIES** frames.

- + 15% of QUIC servers issue AVTs, with sizes between 42 to 86B
- + All tested browsers cache AVTs for the whole browser session

- AVTs are not available on first connect
- Server can enclose arbitrary data into an AVT

Web Tracking Protection

Chrome	Firefox	Brave
Vulnerable	Vulnerable	Vulnerable
Protected	Protected	Protected

Firefox and Brave are isolated (active per origin) to prevent tracking. Local Cookie Protection and Ephemeral Sessions respectively.

- Common third-party page resources (e.g., fonts) benefit most from test handshakes, but are also critical vectors for tracking

Privacy Pass (PP)

Privacy Pass [RFC 9570] enables privacy-preserving authentication.

Instead of presenting linkable state-carrying information to servers (e.g., cookies, AVTs), clients present unlinkable tokens, only sharing one bit of information.

More information can be shared, as specified in the public-reference-secure design, based on PIRGA.

Privacy Pass Address Validation Tokens (PPAVT)

Web Tracking

AVTs can be used for tracking similar to cookies. Currently there is no evidence of AVT trackers.

Embedded third-party visible origin by **Relaxed** header or origin specific URLs.

Cryptography (simplified)

Cryptography is based on **HS256SHA** [RFC 9474] and **draft-ietf-quic-draft-partially-blind-rsa**.

- The browser generates a partially blinded request using the server's public key **pk1**.
 $nonce = random(32)$
 $ext = (ip, lifetime)$
 $blind_sig = bl_blind(pk1, nonce, ext)$
 $req = (blind_sig, ext)$
- The issuer signs the request, after verifying the client's IP and lifetime.
 $blind_sig = bl_blindSig(skt, req)$
 $resp = (blind_sig)$
- The client unblinds the signature, and generates the **SP**.
 $sig = FlexUnblind(pk1, nonce, ext, resp)$
 $token = (nonce, ext, sig, issuer_id)$
- The server verifies the IP lifetime, and signature with the issuer's public key.
 $Verify(pk1, token)$

Testbed

Evaluation

- PPAVT almost reduces handshakes to servers providing AVT
- Verification by Privacy Pass took about 3ms

Open Challenges

- Address reply and double-sending problem
- Enhance browser and I/O origin replication
 - Evaluate the impact of AE-KEM
 - Integrate certificate compression
- Evaluate page load times
- Evaluate more than 3ms top 10
- Cover browsers beyond Chromium
- Optimize PP verification performance

[1] Erik B. Christen-Bauer, Hannes Federrath, and Mathias Fischer. A QUIC Look at Web Tracking. In *PPWT'19*, 29 June 2019, pages 205–206.

[2] Martin Burrows, Puzos-Fotouli Teloni, Raphael Hengen, Jorke Mölck, Thomas C. Schmitt, and Mathias Wählisch. On the interplay between TLS certificates and QUIC performance. In *CoNDOT*, 20 pages 204–211, ACM.