Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

7th May 2019
QUIC Symposium 2019
Diepenbeek, Belgium

Enhanced Performance and Privacy for the QUIC Protocol

Erik Sy

Motivation

- Overhead of the connection establishment presents a performance bottleneck on the web
- QUIC can protect a user's privacy against network observer
- QUIC can contribute to protect the user's privacy against online tracker

Privacy Issues in QUIC's Crypto Handshake

- User tracking via TLS session resumption[1]
- User tracking via gQUIC's server config[2]
- In total, popular web browsers do not sufficiently protect the user's privacy against these tracking mechanisms

[1]: Sy et al: Tracking Users across the Web via TLS Session Resumption, ACSAC'18, San Juan, USA

[2]: Sy et al: A QUIC Look at Web Tracking, PETS 2019, Stockholm, Schweden

Performance Improvements for QUIC's Crypto Handshake

- TLS resumption across hostnames[3]
  - Accelerates connection establishments for an average website by up to 30.6%

- Distributing gQUIC's server config via DNS[2]
  - Saves a round-trip time (RTT) during initial handshakes

[3]: Sy et al: Enhanced Performance for the encrypted Web via TLS Resumptions across Hostnames, Preprint 2019

Visiting the Security of TLS Resumptions across Hostnames

- Security problems are similar to HTTP/2 connection reuse
  - Compare RFC 8336 ORIGIN HTTP/2 Frame
- Attack via an untrustworthy server certificate
  - Adversary leads client to manually accept untrustworthy certificate for captiveportal.com, which is also valid for example.com
  - Client conducts 0-RTT resumption handshake with example.com
  - Passive observer can decrypt the client's request
- Attack circumventing the pinning of server certificates
  - Client resumes to a hostname using a resumption ticket from a connection unrelated to the pinned server certificate

Privacy Issues in QUIC's Transport Handshake

- User tracking via address validation token[2]
- Can we construct tokens with better privacy properties?

Performance Improvements for QUIC's Transport Handshake

- Shared address validation via tokens for future connections[4]
  - Up to 60% of the connections required to retrieve an average website benefit from this improvement
  - Trust relation between server issuing the token and the server consuming the token is validated via the presented x509 certificate

- Shared address validation via out-of-band tokens[5]
  - Every QUIC connection can benefit from this improvement, if the server enforces strict address validation
  - Low-priority tokens because the client does not validate that the issuing server is trusted by the consuming server

[4]: Erik Sy: Surfing the Web quicker than QUIC via a shared Address Validation, Preprint 2019

[5]: Sy et al: QUICker Connection Establishment with Out-Of-Band Validation Tokens, Preprint 2019

Visiting the Scalability of Out-Of-Band Tokens

- Out-of-band tokens are issued via DNS resolver or other QUIC server
  - These entities require a shared secret to issue these tokens
- Key-management needs to be automated via a designated protocol

Future Work

- Only 0.05% of the Alexa Top Million Sites support 0-RTT resumptions[3]
  - Improving the security guarantees of 0-RTT Resumptions[6]

[6]: Aviram et al: Session Resumption Protocols and Efficient Forward Security for TLS 1.3 0-RTT, EUROCRYPT 2019

Conclusion

- The web is slow and we require better protocols to make it faster
- Privacy protections against passive network observers are coming
- User tracking via online services remains a problem

Thank you

Questions and Answers

E-mail: quic@erik-sy.de