QUIC
Human Rights Review

Beatrice Martini, Harvard University
Niels ten Oever, University of Amsterdam

HRPC Human Rights Review Team

IETF 102
July 19 2018, Montreal

QUIC (Quick UDP Internet Connection)

New multiplexed and secure transport atop UDP, designed from the ground up and optimized for HTTP/2 semantics.

Key features of QUIC over existing TCP+TLS+HTTP2 include:

- Dramatically reduced connection establishment time
- Improved congestion control
- Multiplexing without head of line blocking
- Forward error correction
- Connection migration

Research focus and goals

Review of the following QUIC drafts:

- draft-ietf-quic-transport-13
- draft-ietf-quic-tls-13
- draft-ietf-quic-invariants-01

Desired outcomes:

- Improved relevance and quality of examined QUIC drafts
- Increased experience with other methods to conduct Human Rights Reviews
- Mainstreaming Human Rights Reviews in the IETF

Selected early finds

Connectivity

- Improves connectivity on low latency and high loss connections
- Strengthens end-to-end encryption
- Addresses ossification (the inability to deploy new protocol or protocol extensions due to the unchangeable nature of infrastructure components that have come to rely on a particular feature of the current protocols)
    - Transport headers are encrypted. Encryption prevents ossification of the protocol by middleboxes, which can't make routing decisions based on information they can't understand
    - Greasing: the QUIC packet format is designed to allow future changes to the protocol

Selected early finds

Privacy

- Creates higher opacity for the observer by establishing connection with multiple streams
- Decreases linkability through the use connection ID in case of connection migration
- Proposed: Padding, which would help to evade traffic analysis for protected packets
- Proposed: Addition of a "latency spin bit" to the QUIC short header, for explicit passive measurability of the protocol

Selected early finds

The spin bit is a bit in the header that flips once a round trip, so that observers can estimate RTT, designed for explicit passive measurability of the protocol.

> Example of argument against it: It reveals information on the locality of the end points
>
> Example of argument in its defense: Since it is decoupled from the application’s state, it does not appear to leak any information about the endpoints, beyond an extremely rough estimate of location on the network

Selected early finds

Security

- Improvement: QUIC integrates security directly into the transport protocol, instead of on top of it
- By enforcing end-to-end encryption, QUIC hinders connection hijacking attacks and passive surveillance
- By adding more privacy and more functionality together in one protocol, there is a risk for networking to become more opaque, and therefore harder to secure and analyze

Selected early finds

Internationalization

- draft-ietf-quic-transport states that the Reason Phrase in the CONNECTION_CLOSE and APPLICATION_CLOSE frames "SHOULD be a UTF-8 encoded string [RFC3629]", but there is no language definition set

Selected early finds

Censorship resistance

- End-to-encryption makes monitoring harder, thus improving censorship resistance
- If implemented, the spin bit could create the following issues:
    - By revealing information regarding the locality of the end points from each other, it could be used by the operator to discriminate over traffic flows
    - The operator would recognize when a user is using a tunnel when migrating connection, and could decide to create access issues

Selected early finds

Outcome transparency

- Power shift: From the network operators, to the end points.
- Architectural consideration: The server can set several conditions, including what conditions the client is able to set. This makes it harder to compare the services that are provided to the client, and the reasons behind it (including AI, machine learning). In this sense, QUIC can hinder the analysis of non-discrimination of users

Questions or feedback?

mail@beatricemartini.it

mail@nielstenoever.net

ietf.org/mailman/listinfo/Hr-rt