Analyzing Quic in the wild

While Quic is still specified by the IETF [1], a lot of implementations exist [2] and as shown by related work [3] deployment is on the rise. A major goal of Quic is to combine a fast connection establishment, with reduced overhead and early encryption. Therefore, it is build on UDP and directly incorporates TLS. UDP provides a lightweight transport protocol with widespread compatibility in network devices, while TLS, majorly version 1.3, provides state-of-the-art encryption and 0-RTT or 1-RTT handshakes. This makes the analysis of configurations and real-world behavior based on passive traffic captures nearly impossible. Thus, a proper analysis requires active scans.

While Rüth et al. [3] focus on the detection of Quic deployments and seen versions, this work focuses on the analysis of deployed devices and their behavior in a stateful approach.

- Implement and set up Quic scans
- Analyze different input sources
- Analyze the behavior of targets and differences to a TLS + TCP setup

Basic programming knowledge in Python or Go
Familiarity with GIYF-Based work approaches

Bibliography

Contact
Johannes Zirngibl  zirngibl@net.in.tum.de
Patrick Sattler   sattler@net.in.tum.de
Benedikt Jaeger   jaeger@net.in.tum.de
https://net.in.tum.de/members/zirngibl/