Evaluating Different QUIC Scan Approaches

In May 2021 QUIC was finally specified by the IETF [1], a lot of implementations exist [2] and as shown by related work [3,4], 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 builds 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. This work focuses on the evaluation of different QUIC scan approaches, a setup of a local test environment including different server implementations and targeted Internet scans.

Motivation

- Setup a local test environment including different QUIC servers
- Design and evaluate different stateless and stateful QUIC scan setups/configurations
- Identify sources of errors
- Evaluate the impact on targeted Internet Scans

Your Task

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

Requirements

Bibliography


Contact

Johannes Zirngibl  zirngibl@net.in.tum.de
Patrick Sattler  sattler@net.in.tum.de

https://net.in.tum.de/members/zirngibl/