Privacy-preserving Explicit Network Support

Mirja Kühlewind; Simone Ferlin; Marcus Ihlar

Ericsson research, E-mail: first.last@ericsson.com

Abstract. With the advent of QUIC, a new and fully encrypted transport protocol, as well as the increase in deployment of TLS 1.3 in HTTP/2, end-to-end encryption becomes the default in the Internet. In particular, QUIC has been developed with focus on minimising information exposed to the network in order to reduce potential privacy risks, but also avoid unwanted interference from network devices on the end-to-end path.
However, the fact is, that today's network management is more than just merely traffic forwarding. Networks can offer improved services that help optimising traffic given certain network characteristics, e.g. cellular or satellite links. As a matter of fact, Performance Enhancing Proxies (PeP) are nowadays mostly operated transparently to the endpoint by relying on exposed traffic information available on different layers. While this approach was straightforward to realise and it successfully enabled enhancements to both, network utilisation and user experience, in some cases, with the increase in end-to-end encryption it can no longer be sustained. This talk discusses solutions that explicitly enable endpoints to request network support and provide an encrypted and authenticated communication channel with an intermediate network device, supporting performance enhancing services, if explicitly requested, in a privacy-preserving way.
We assume the setup shown in Figure 1, where the client opens a QUIC connection to the proxy and sends a HTTP CONNECT request. As proposed by MASQUE [1], this QUIC connection is converted into an authenticated tunnel, where at least one of the QUIC streams can be used as a communication channel between client and proxy. The client can then instruct the proxy to open another QUIC (or also TCP) connection to one or multiple servers and forward traffic of selected streams. Optionally, an end-to-end encrypted channel between client and server can be set up, enabling even encrypted and authenticated communication towards the server.

Keywords: Proxy, QUIC, encryption, TLS, tunnel

References

1. D. Schinazi, The MASQUE (Multiplexed Application Substrate over QUIC Encryption) protocol, https://tools.ietf.org/html/draft-schinazi-masque

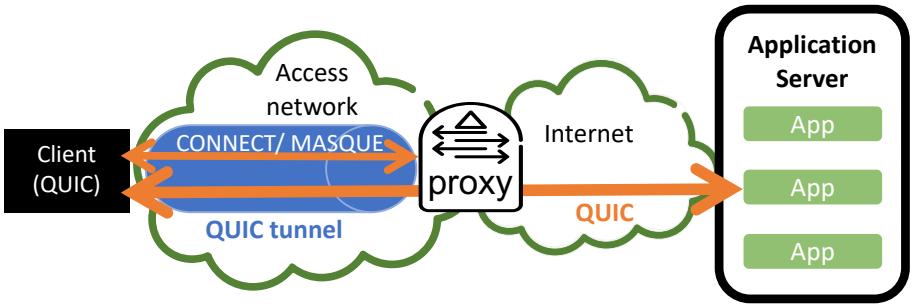

Fig. 1. Tunnelling with QUIC and MASQUE.