MASQUE

draft-schinazi-masque
draft-schinazi-httpbis-transport-auth

IETF 105 – Montreal – 2019-07

David Schinazi – dschinazi@google.com

MASQUE

Multiplexed Application Substrate over QUIC Encryption

Run multiple applications over a QUIC connection that looks like HTTP/3

Use-case: build a QUIC proxy

- Hide network traffic from network provider
- Hide client location from web servers
- Provide access to a home server
- Onion routing / Tor over QUIC?

HTTP Transport Authentication

Moved to its own document since Prague: draft-schinazi-httpbis-transport-auth

Unidirectional authentication of client to server

```
Transport-Authentication: Signature u="am9obi5kb2U=";a=1.3.101.112;
   p="SW5zZXJ0IHNpZ25hdHVyZSBvZiBub25jZSBoZXJlIHdo
   aWNoIHRha2VzIDUxMiBiaXRzIGZvciBFZDI1NTE5IQ=="
```

Server can hide that it supports this mode of authentication

Supports asymmetric keys or shared secret

Authentication tied to underlying transport via TLS key exporter

QUIC Proxy

Client establishes QUIC connection to MASQUE server

Client establishes second QUIC connection through the first one to Web Server

Leverages QUIC DATAGRAM frames

MASQUE server does not have access to end-to-end encrypted content

QUIC Proxy – Port Sharing

MASQUE server can multiplex outgoing connections on UDP/443 instead of using one ephemeral UDP port per outgoing connection

Leverage QUIC client connection IDs

MASQUE server imposes requirements on client's use of client connection IDs

Ability to compress IP addresses, ports and connection IDs

Quic Proxy – Nested Congestion Control

QUIC DATAGRAM frames are subject to congestion control

End to end data will be subject to two congestion controllers

However: outer one does not retransmit: better performance than TCP over TCP

Conceptually outer congestion controller is akin to any router

MASQUE Control Protocol

Server needs a mechanism to tell the client what services it offers

Not currently defined

MASQUE

draft-schinazi-masque
draft-schinazi-httpbis-transport-auth

IETF 105 – Montreal – 2019-07

David Schinazi – dschinazi@google.com