QUIC Protocol: DoS attack

Anomaly Detection

Maria Inês Rocha 93320

Pedro Abreu 93240

TPR - November 2022

QUIC Overview

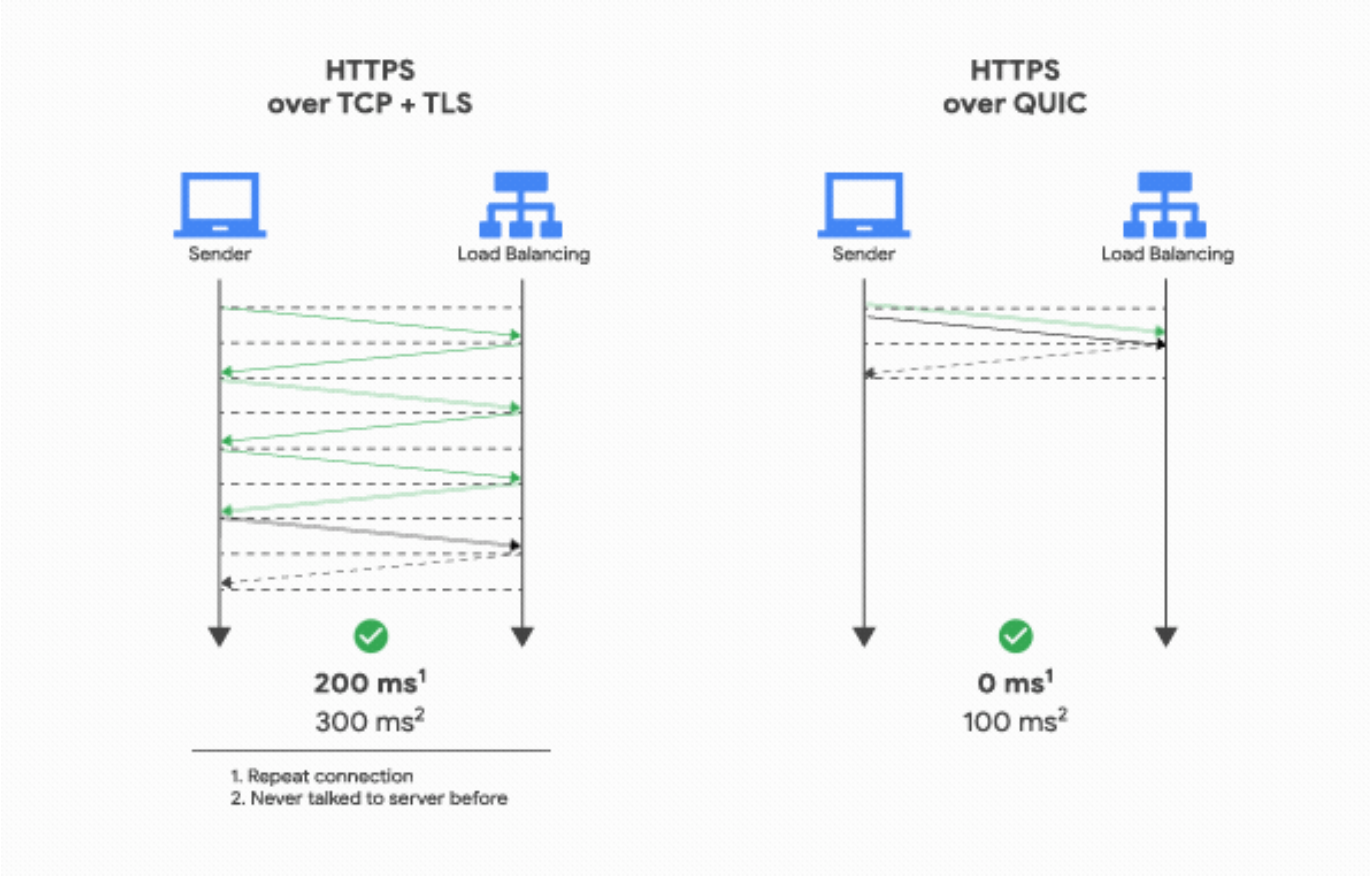
- New internet transport protocol developed by Google

- Objectives:
  - Faster (latency reduction)
  - More efficient
  - More secure
  - Evolvable

- 0-RTT feature

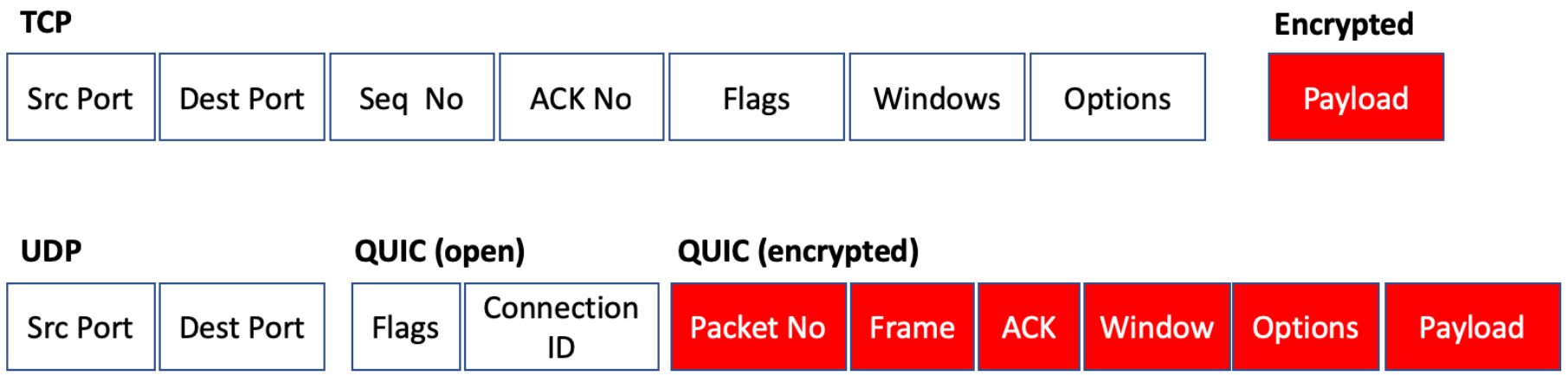
- **Encrypted** packets

- Over **UDP**



Security Problem

- **QUIC DoS attack** – service denial attack
- Hard to handle:
  - UDP packets with few information
  - QUIC encrypted packets analysis



Solution Relevance

- ✓ Distinguish regular from malicious users
- ✓ Increasing the reliability
- ✓ Protocol popularity is growing, so will the attacks to it

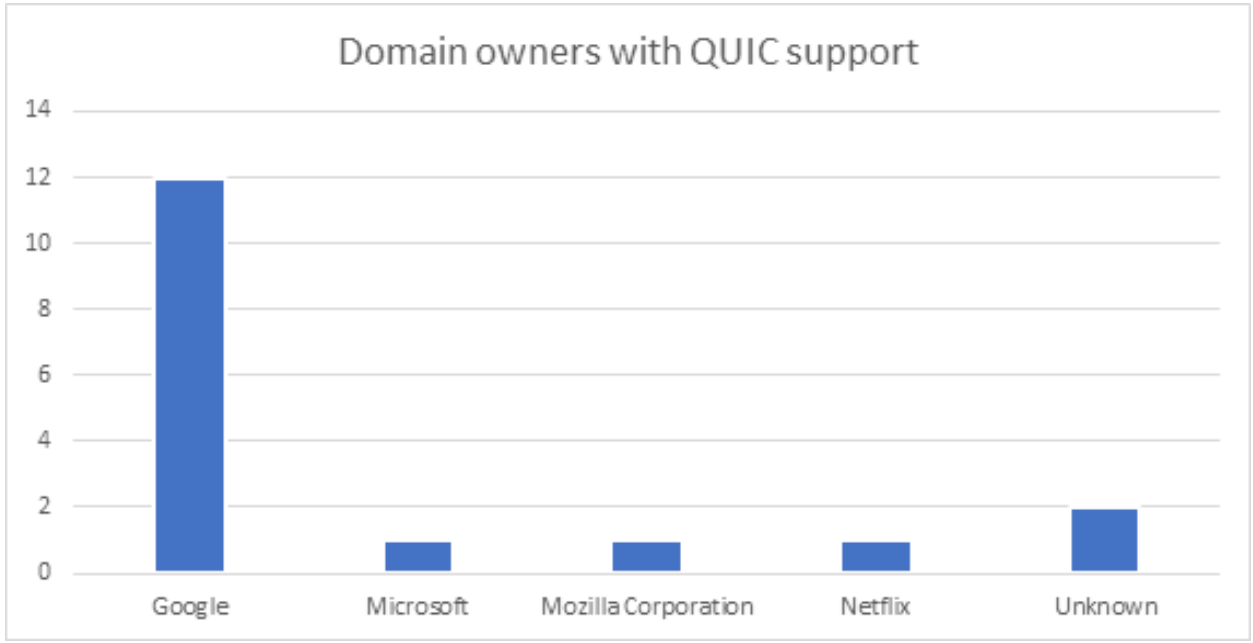
- Service downtime affects:
  - ➢ The clients
  - ➢ The image
  - ➢ The business/profits
  - ➢ Performance decreasing

Solution Relevance

Emerging Threats Target App Devs, Gamers

April 2021 Cloudflare Reports

The report also detailed the rapid rise of three emerging threat vectors. These targeted Jenkins and TeamSpeak3 servers, as well as the quick UDP internet connection (QUIC) protocol, which grew 940%, 203%, and 433%, respectively, quarter over quarter.



KeySight Blog Jan 2022

8 April 2021

The quantity and power of DDoS attacks in 2021 will increase significantly

StormWall Blog

Updated: Nov 4, 2022

Distributed denial-of-service (DDoS) attacks have been a continuous threat since the advent of the commercial internet. The struggle between security experts and DDoS protection is an asymmetrical war where $30 attacks can jeopardize millions of dollars for companies in downtime and breaches of contract.

By Stephen Condon, Kentik

Data Sources

Network Packets

- Wireshark

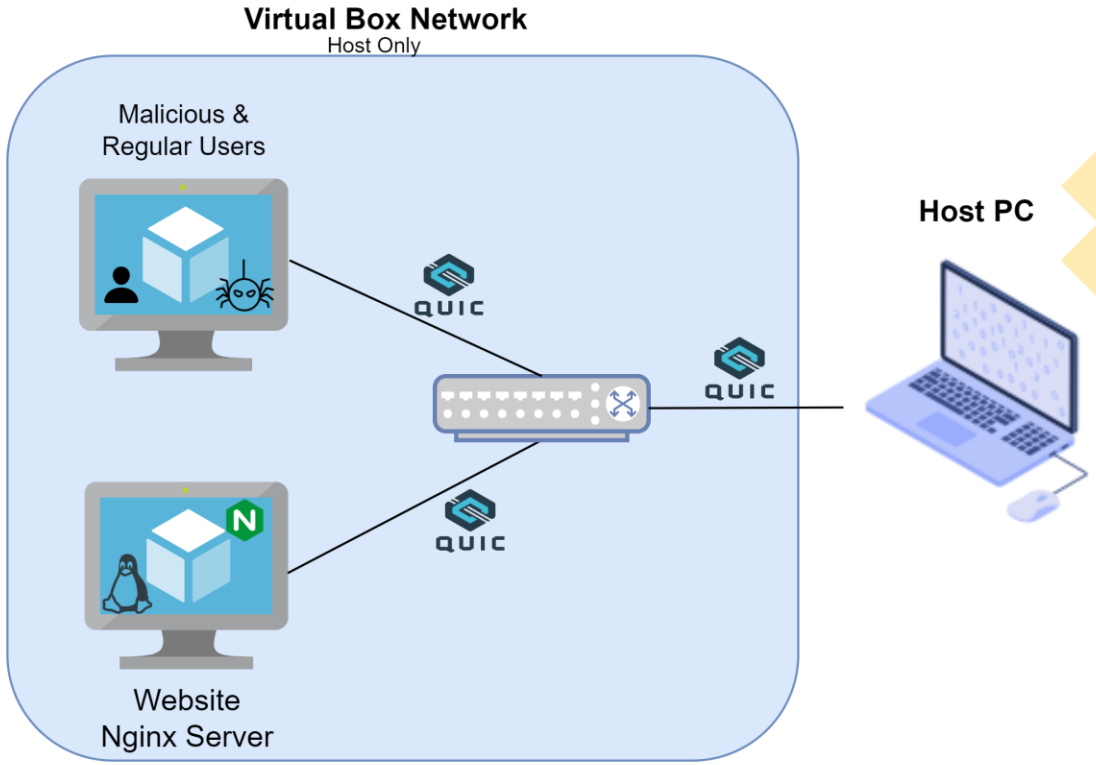
Observation Window

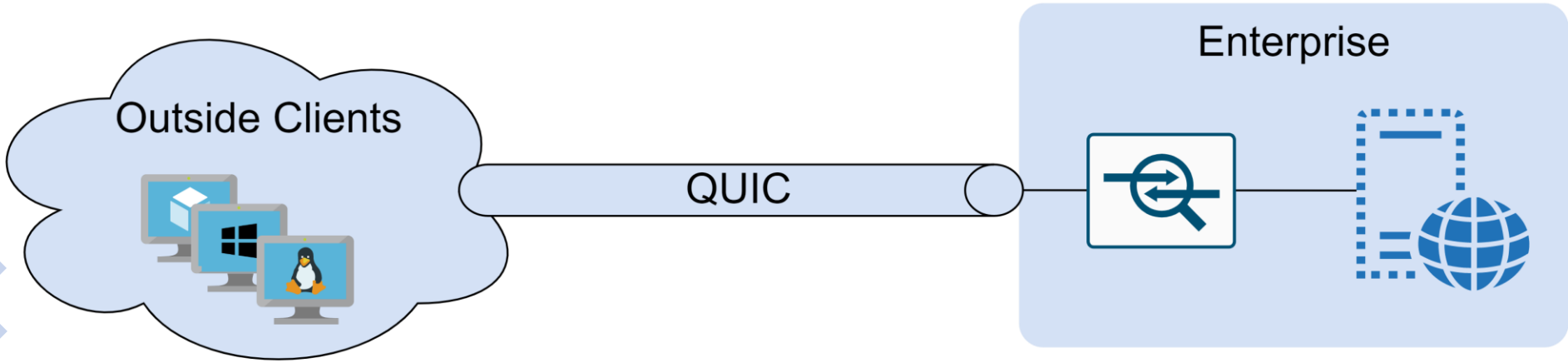
- 1 minute and 30 seconds
- Sliding of 20 seconds

Captures performed in public QUIC supporters:

Snapchat	• Video, image, buttons, forms • Duration: 15mins
Instagram	• Video, image, buttons • Duration: 15 mins
unter.com.tr	• text, browsing • Duration: 5 min

Solution Setup & Real World Scenario

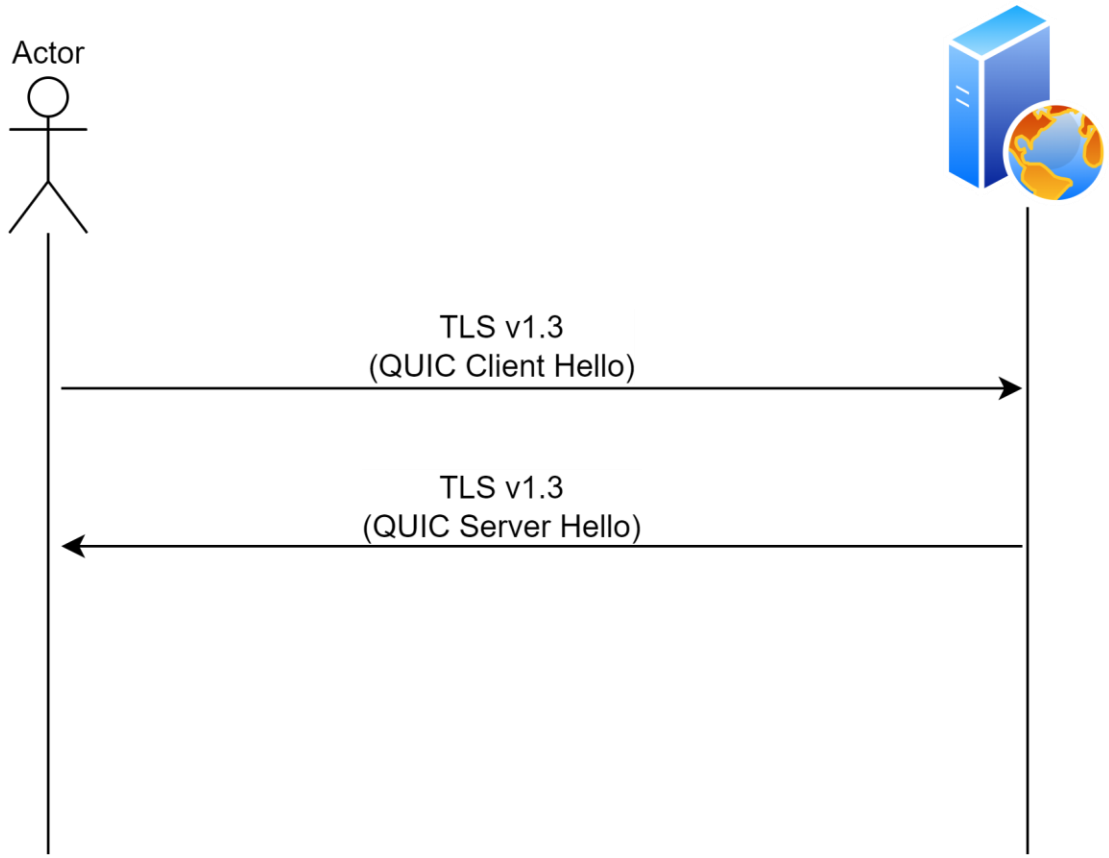




Test Scenario 1

Incomplete Handshake

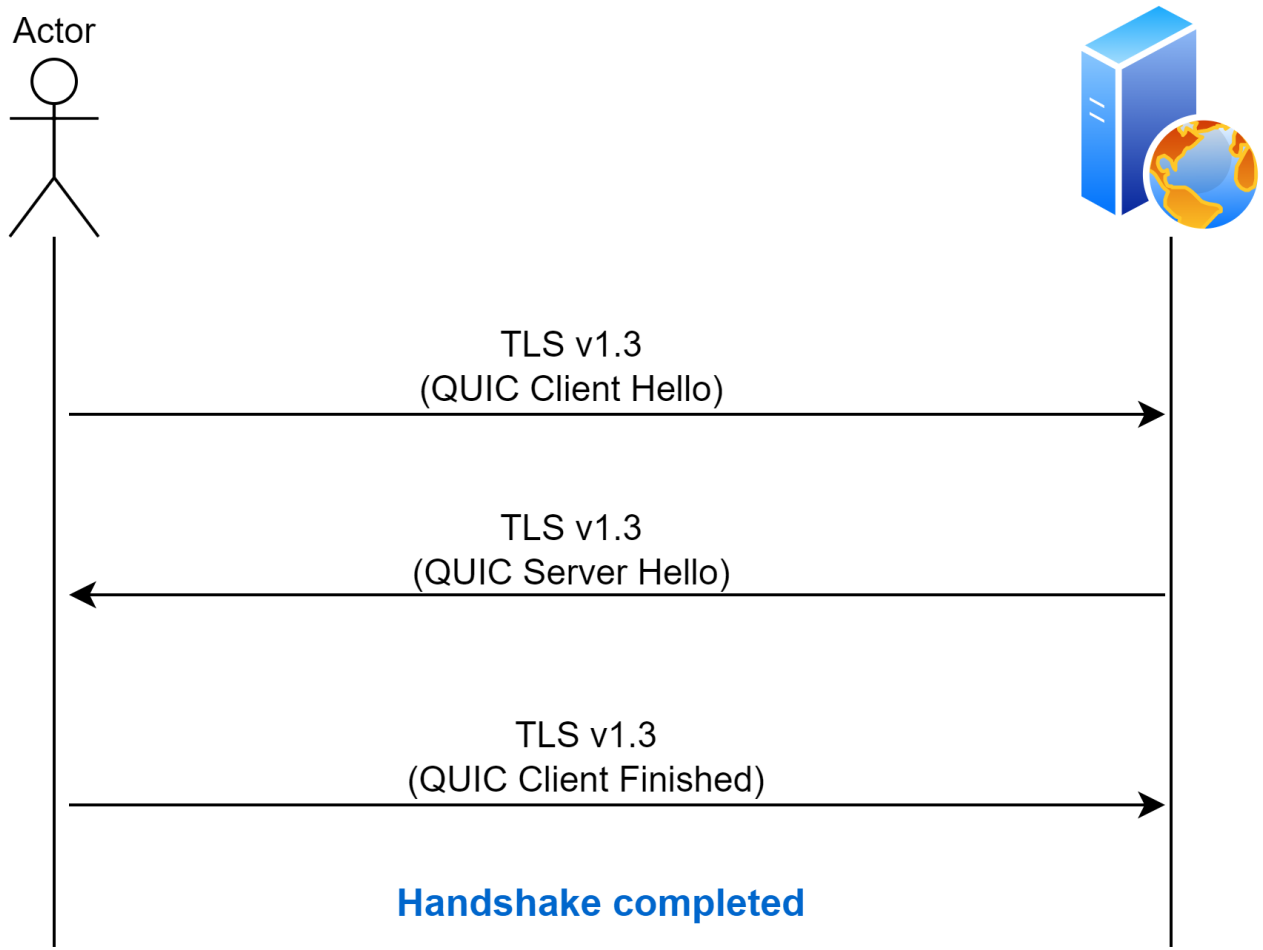
After the server response, the attacker doesn't send the finished handshake message.



Test Scenario 2

0 data packets exchanged

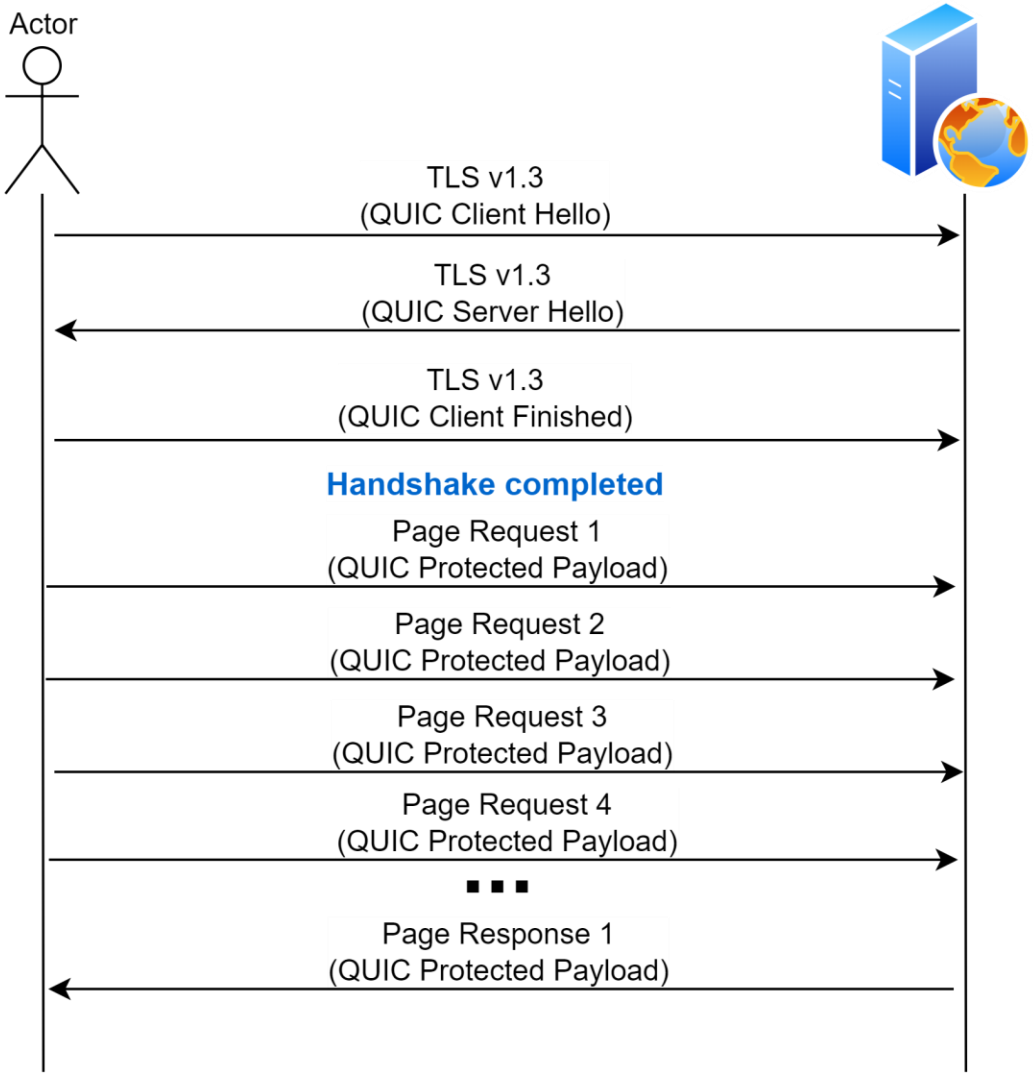
After the handshake is completed, no more data is exchanged.



Test Scenario 3

Requests Overload

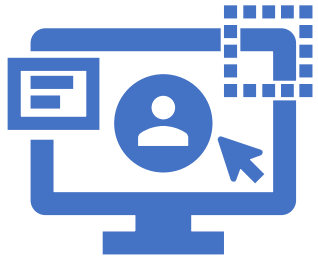
The number of requests sent by the actor is much higher than a regular actor interaction.



Metrics

Source IP
Destination IP
Packet Size
Number of QUIC Initial Packets (TLSv1.3 Client Hello)
Number of QUIC Initial Packets (TLSv1.3 Server Hello)
Number of QUIC Initial Packets (TLSv1.3 Client Finished)
Number of QUIC Packets (Protected Payload)

Features



QUIC Initial (TLS1.3 Client Hello)

Activity periods:

- number, average time, standard deviation

Silent periods:

- number, average time, standard deviation

QUIC Client Finished

Activity periods:

- number, average time, standard deviation

Silent periods:

- number, average time, standard deviation

Features

QUIC Protected Payload

Number of packets pushed from server to client

Number of packets pushed from client to server

Total number of packets in a flow

Minimum packet length

Maximum packet length

Average packet length

Median packet length

Mode packet length

Standard deviation packet length

95th percentile packet length

Activity periods:

>> number, average time, standard deviation

Silent periods:

>> number, average time, standard deviation

QUESTIONS?

Thank you for your attention!