MECT | Network Awareness Techniques

# QUIC DDoS Attack mitigation

## Malicious actor detection

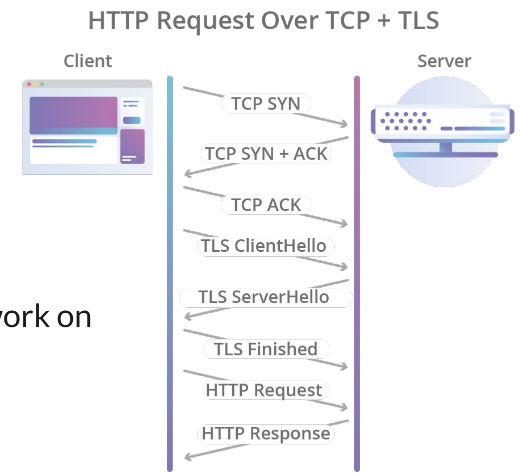
By Jodionísio Muachifi (97147) and Rúben Castelhano (97688)

Teacher:
Paulo Jorge Salvador Serra Ferreira

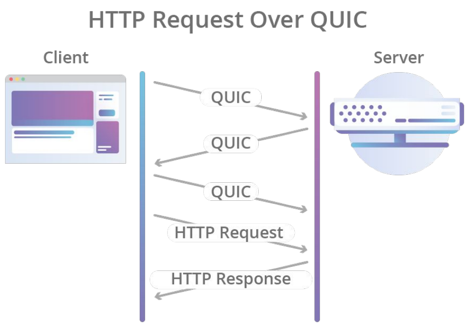
November 2023 | 1st Presentation

# QUIC Overview

- Modern transport protocol developed by Google
  - Development began at Google in 2012 aiming to overcome some limitations of TCP
  - Publicly announced and open-sourced by Google in 2015
  - The Internet Engineering Task Force (IETF) took an interest in QUIC and decided to work on standardizing it
  - In 2018 the IETF published the first drafts of the protocol
  - In 2019 QUIC became the transport protocol for HTTP/3
  - Officially standardized in August 2021 as RFC 9000




- Main advantages over TCP (QUIC+HTTP/3 vs TCP+TLS+HTTP/2)
  - Faster handshakes
  - Improved congestion feedback
  - Multiplexing without head-of-line blocking
  - Built-in security
  - Connection migration support
  - Optional unreliable or partially reliable delivery



# The problem - 1

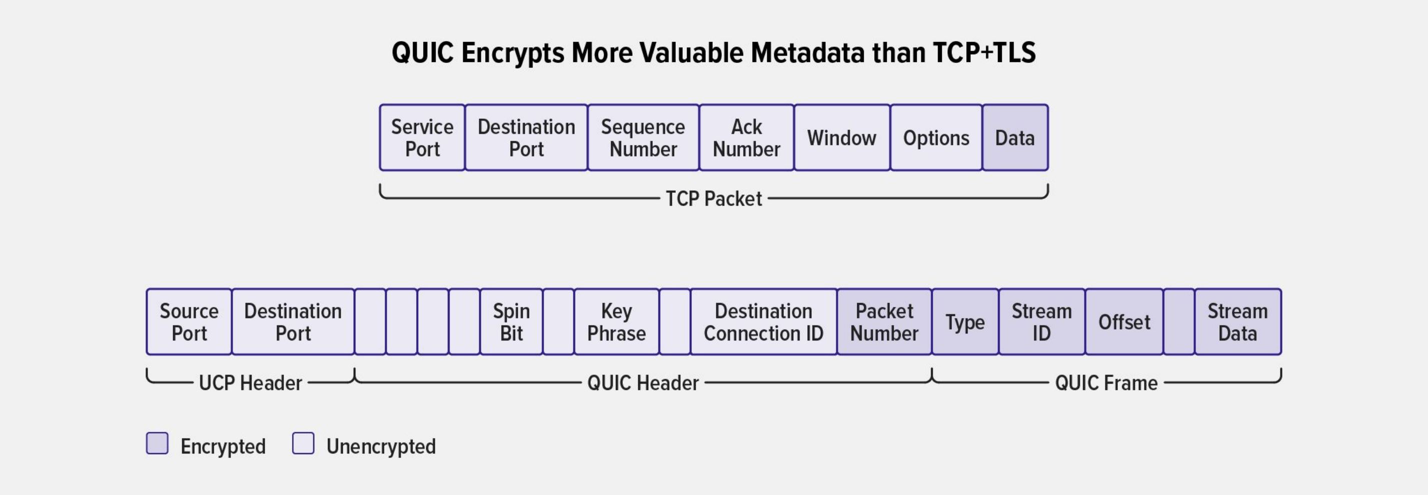
- DDoS attacks present serious problems for businesses:
  - Lost revenue
  - Decreased customer trust and reputation loss
  - Service unavailability is not permissible in certain fields (finance, health, military, etc.)
  - A pure brute-force defence is extremely expensive
  - Blocking access to the service is essentially letting the attacker win, since service unavailability is still achieved

- The average amount of downtime following a DDoS attack is 54 minutes and the average cost for each minute of downtime is $22,000[1]

1. Ponemon Institute, “Cyber security on the offense: A study of IT security experts”, November 2012

# The problem - 2

- Mitigating a traditional TCP DDoS attack is hard
  - Packet analysis is of limited use since payloads are encrypted
  - Crucially, the TCP header is left unencrypted
- Mitigating a QUIC based DDoS attack is harder
  - Encryption extends beyond just the payload; the majority of protocol fields are also secured



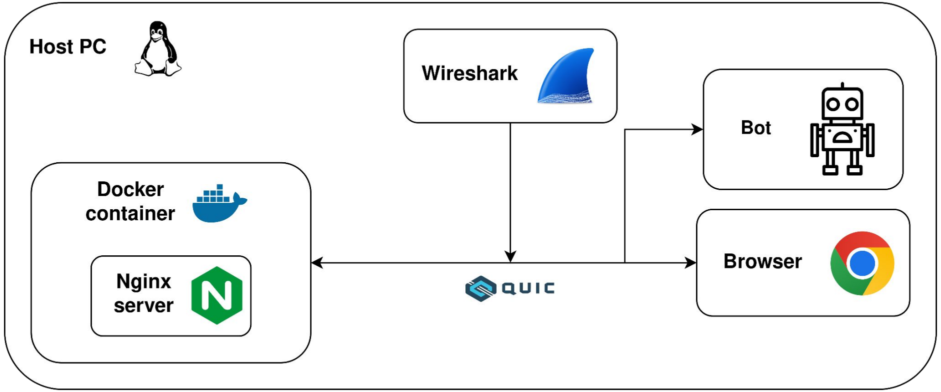
# Our focus

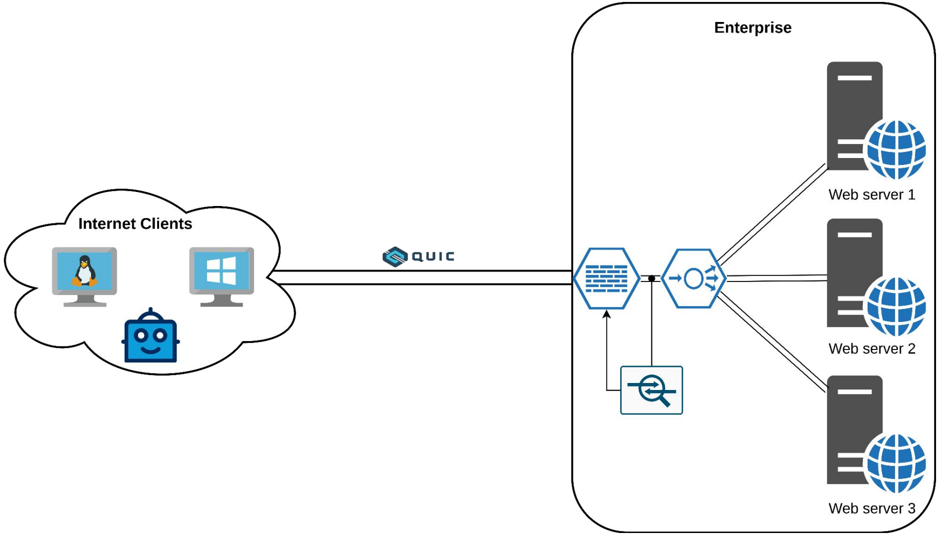
- A proper DDoS mitigation solution is complex and based on several levels of detection and prevention:
    - Stateless firewalls blocking known bad actors
    - Load-balancers
    - Resource and network monitoring
        - **Distinguish between regular and malicious users** **<--- this will be our focus**

- We will monitor the network traffic patterns of known good actors to understand how they use a service to distinguish them from several levels of attackers

# Data sources and real-world scenario

- We plan to build a simple, mostly reading based website (with some images/video content as well) and serve it in HTTP/3 via NGINX
- Capture packets using Wireshark



# Test scenarios

- Basic Bot
  - Does not attempt to mask its behaviour
  - Spams requests indiscriminately
- Intermediate Bot
  - Badly attempts to mask its behaviour
  - Random intervals with a fixed distribution and variance
- Advanced Bot
  - Attempts to mask its behaviour
  - Imitates regular user behaviour and human timings

# Data processing

- Collect raw packet data with a sampling period of 0.01 seconds
- Filter data to allow only QUIC packets between the clients and the web server
- Aggregate data by client (source IP address)
- Detect anomalous user behaviour

Observation process:

- Multiple sliding windows
    - 30 seconds and 3 minutes long
    - sliding every 5 seconds

# Extracted features

- Number of download/upload packets
  - mean, median, variance, stdev
  - min, max
  - 99th, 98th, 95th, 1st, 2nd, 5th percentiles
  - covariance (between download and upload)
- Download/upload packet size
  - mean, median, variance, stdev
  - min, max
  - 99th, 98th, 95th, 1st, 2nd, 5th percentiles
  - covariance (between download and upload)
- Periods of silence
  - mean, median, variance,  stdev
  - min, max
  - 99th, 98th, 95th, 1st, 2nd, 5th percentiles

**Thank you for your attention!**
**Any questions ?**

# References


- https://peering.google.com/#/learn-more/quic
- https://blog.cloudflare.com/the-road-to-quic/
- https://www.nginx.com/blog/primer-quic-networking-encryption-in-nginx/
- https://nsfocusglobal.com/wp-content/uploads/2017/01/Distributed_Denial_of_Service_Attacks__An_Economic_Perspective__Whitepaper.pdf