
Fingerprinting schemes against a Post-Quantum Cryptography IPsec/IKEv2 Encryption appliance

Master's thesis



About NQX

The need for a quantum-safe encryption appliance

- Quantum Computers – threat towards Public Key Cryptosystems used in online communications
- Attacks against key exchange – recover the session keys used for encrypting data
- Long term confidential data compromised

NQX

- Protects critical data in transit from unauthorized access
- High-performance rule-based packet forwarding and filtering
- Quantum safe encryption for L2 (data link layer) and L3 (IP network) data transport
- PQC Algorithms for key exchange methods(IKEv2)
 - Crystals-Kyber, SABER, and NTRUEncrypt as part of hybrid key exchange
- Centralized management with comprehensive GUI

Problem Statement

Motivation: VPNs must not leak useful information about the utility traffic they protect.

Goal: The aim of this thesis is to determine if a passive observer of VPN traffic can find useful information about the protected data, communicating parties, or applications/devices being used in the communication.

Product tested: NQX – L3 VPN

Lab setup

Network topology – NQX configuration and Installation

Experiments – Data Collection

Website fingerprinting – SSH sessions – File transfers

Data Analysis

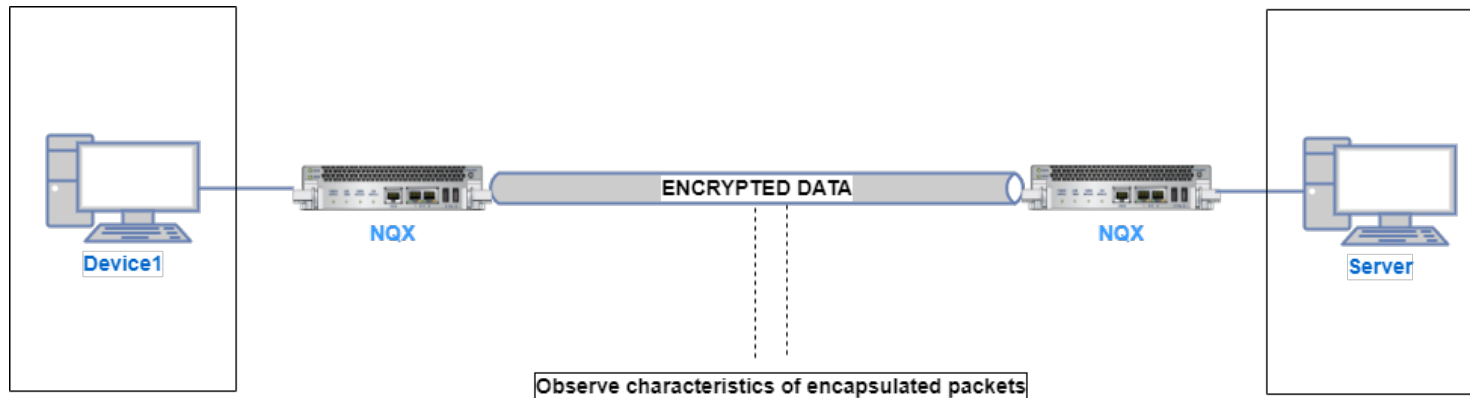
Graphs – Correlation analysis

Results

Evaluation – Conclusions

Experiments

Link data captured - ESP packets filtered - Packet features (length, timestamp) extracted and analyzed



Website fingerprinting:

- Device1 sends HTTPS requests via the VPN tunnel to Server which acts as the gateway to the internet

SSH session:

- SSH connection from Device1 to Server
- Testing active interactions using text editors

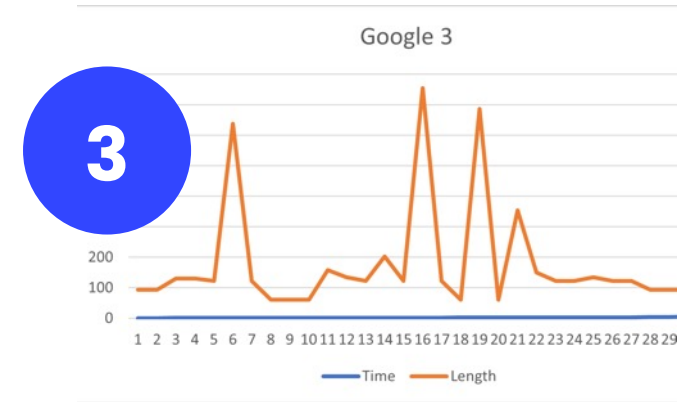
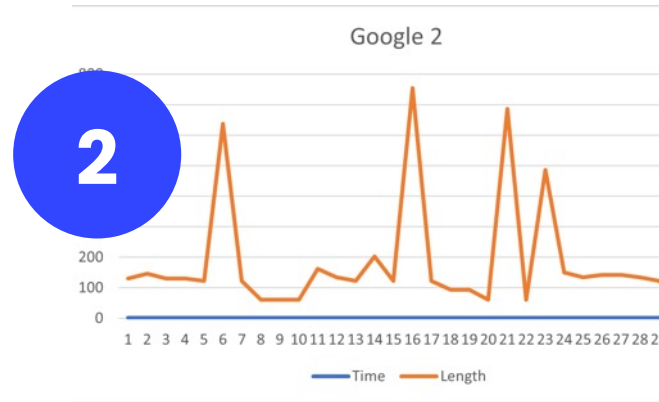
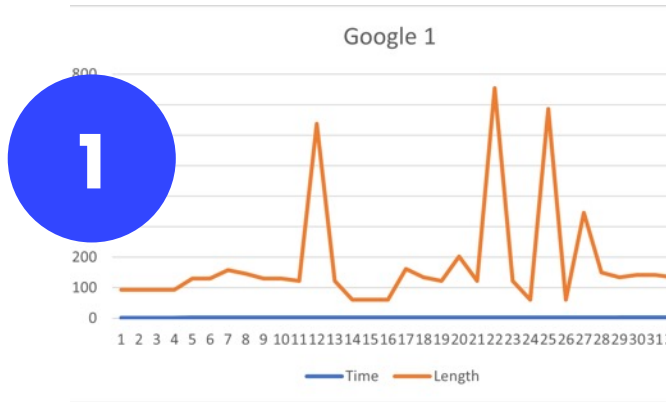
File transfers:

- Testing transfer of small and large files with random data from Device1 to Server using SCP

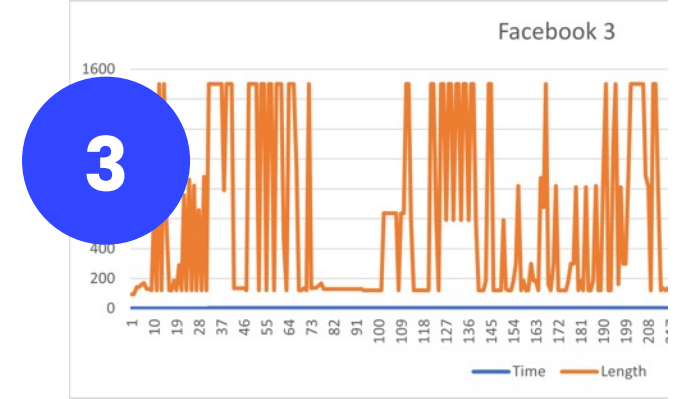
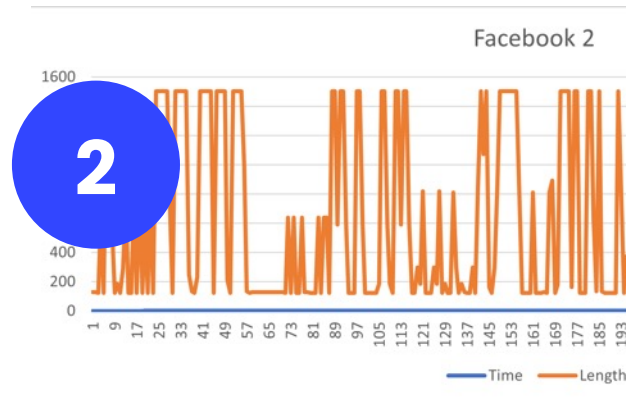
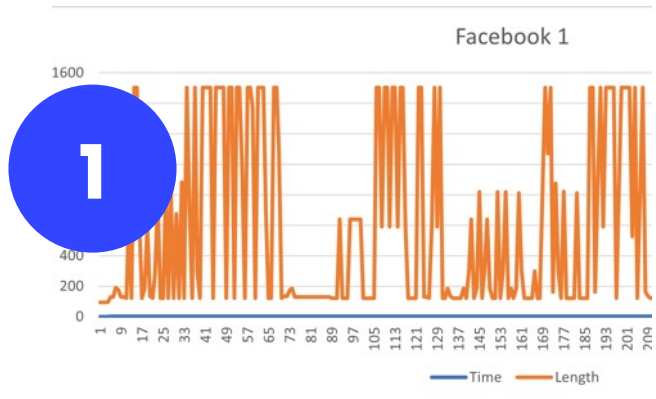
Website homepage fingerprints



Google



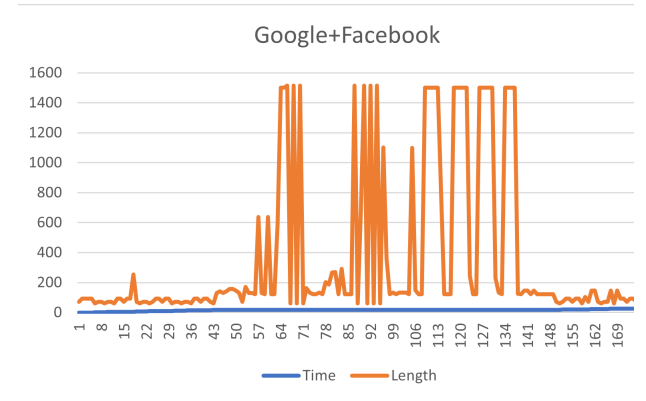
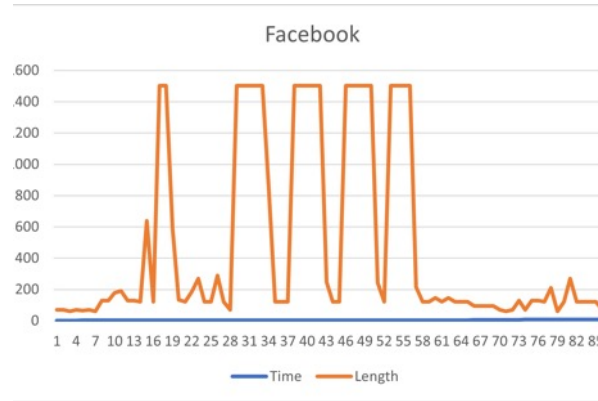
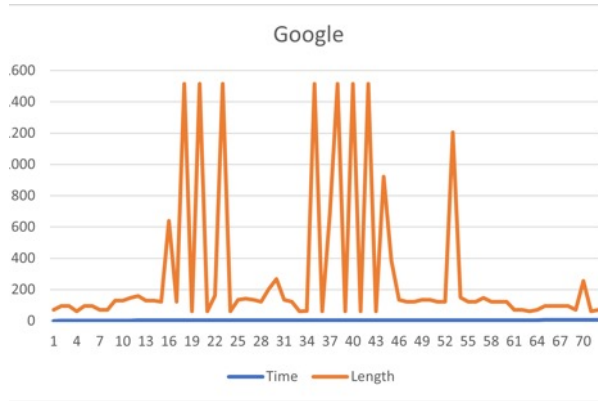
Facebook



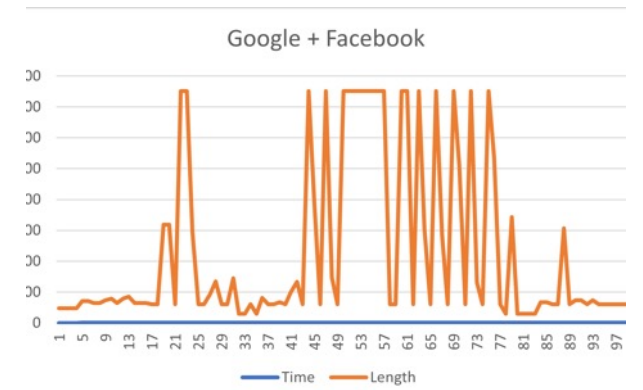
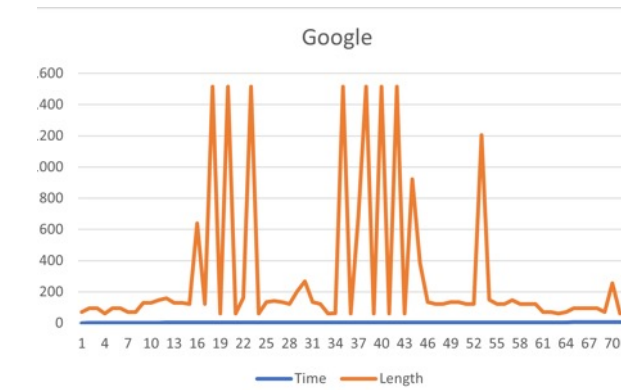
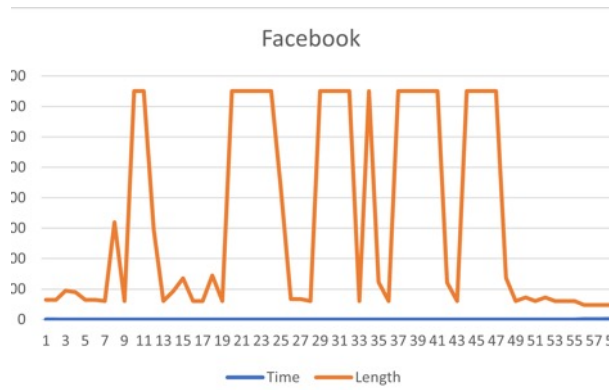
Multiple websites simultaneously



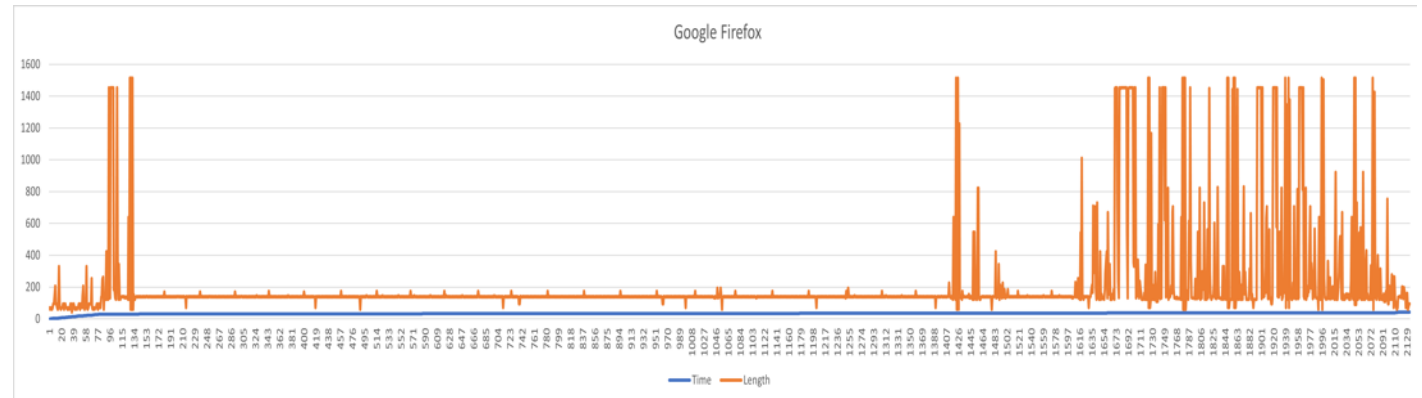
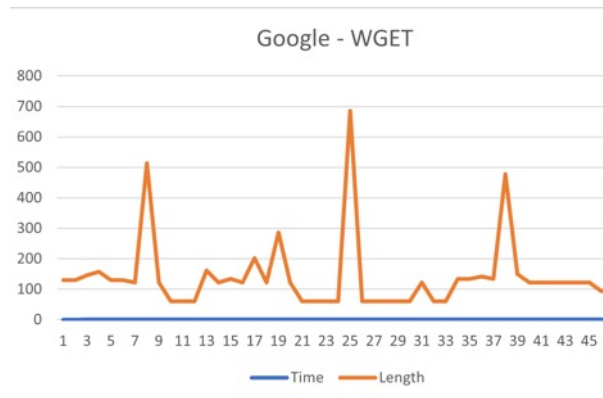
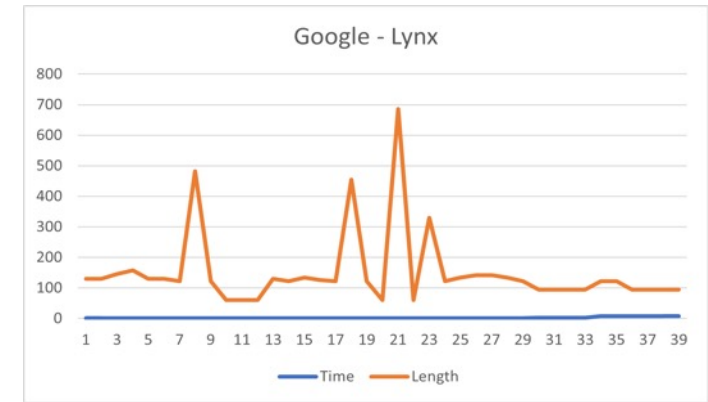
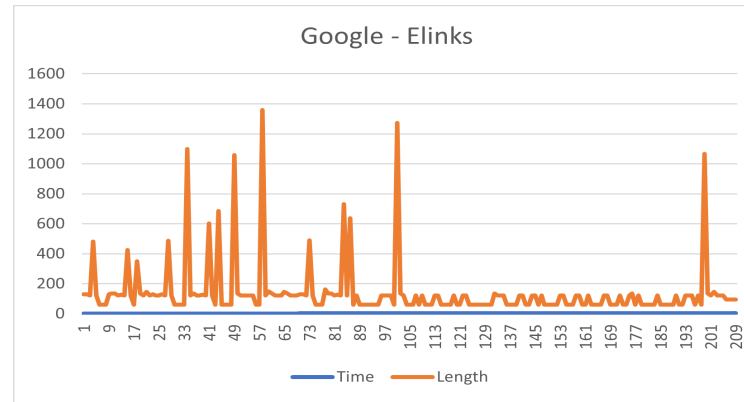
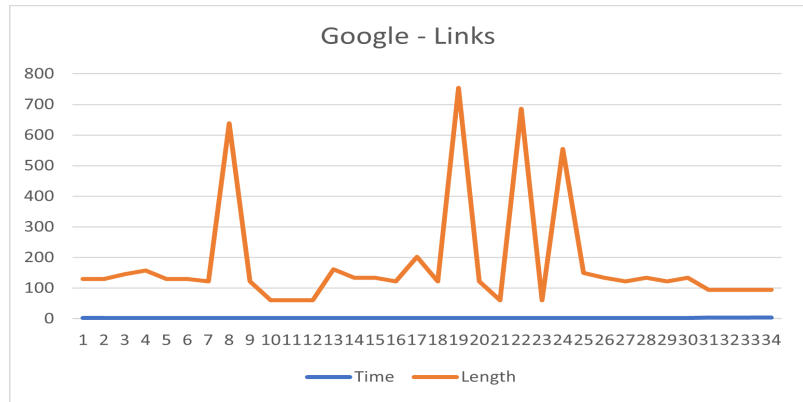
Google + Facebook



Facebook + Google



Different browsers and tools



Data Analysis

- To find the correlation between the data samples collected
- To be able to classify the new samples based on existing fingerprints
- Factors under consideration:
 - Total number of packets in a sample
 - Time lag between packets
 - Number of peaks(large packets)



**Static vs Dynamic
website content -
Fingerprints change**

Evaluation

- Though the PQC algorithms ensure confidentiality, they don't hide data traffic patterns
- Fingerprints of websites or applications can be obtained and used for predicting information about the data in transit in the future.