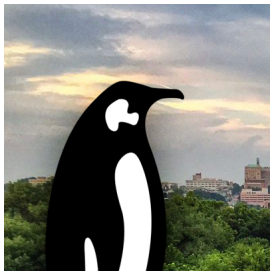

Contribution ID: **288** Type: **not specified**

Offloading QUIC Encryption to Enabled NICs

Wednesday, 15 November 2023 12:00 (30 minutes)

In large deployments, significant CPU cycles are used on encryption for transport security (QUIC, TLS, etc). CPU crypto instructions and 'look-a-side'accelerators can have significant performance penalties (memory copies, cache pollution, etc).

NIC or Inline offload solves many of these problems and it leverages the natural memory copy into the NIC to implement crypto-offload. Other protocols (kTLS, IPSec) have been successfully offloaded using this technique, it is time for QUIC to do the same.

This presentation will cover the software design (from userspace to hardware driver) for utilizing crypto offload for QUIC packets using offload capable NIC implementations (including future Broadcom NICs). In addition to covering the design and implementation of this infrastructure there will be discussion around the performance benefits to this solution to those that want to utilize QUIC offload in their infrastructure.

Primary author: GOSPODAREK, Andy (Broadcom)

Presenter: GOSPODAREK, Andy (Broadcom)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track