UbiCrypt

Trustworthy Encryption Everywhere

Ofir Weisse, Tim Trippel, Jeremy Erickson

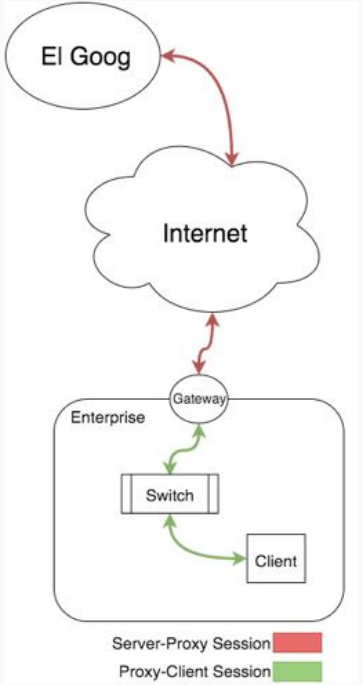
Motivation

- Ubiquitous Encryption
  - “HTTPS Everywhere”
  - Let’s Encrypt
- Enterprise security policy requirements
  - Network introspection
    - Auditing
    - Intrusion Detection
    - Parental Controls

CONFLICT

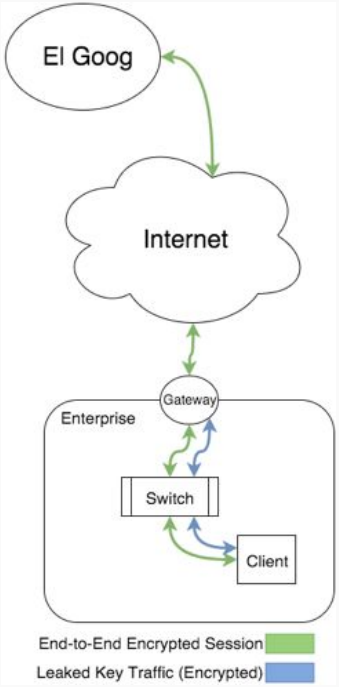
What’s Wrong - TLS Splitting

- Violates principle of E2E security
- Gateway & client may trust different Root CA sets
  - {GA} > {CL} : Client may connect to server it does not trust
  - {GA} < {CL} : Gateway cannot authenticate server:
    - Gateway blocks client connection
    - Gateway degrades security



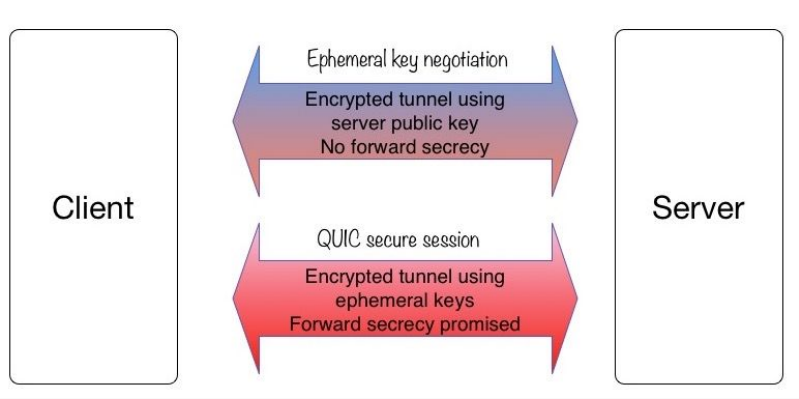
UbiCrypt to the Rescue

- Allow E2E connection between client and server
- Client securely leaks session key to gateway
- Gateway can introspect on traffic
- Implementation
  - Modify QUIC on client
    - Application layer
    - New - accepting changes
    - No modification of server necessary → DEPLOYABILITY
  - Add gateway support



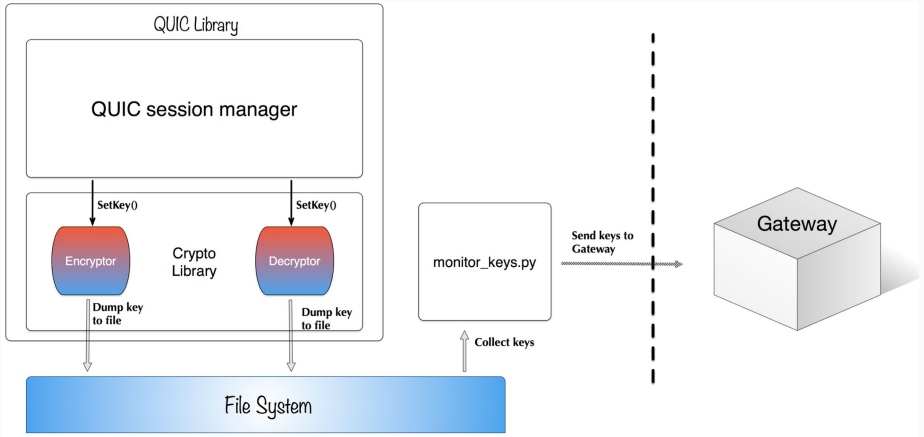
QUIC Overview

- Connection establishment phases:
  - Ephemeral key negotiation
    - Retrieve server public key
    - **Negotiate ephemeral keys**
  - Setup forward secret secure session



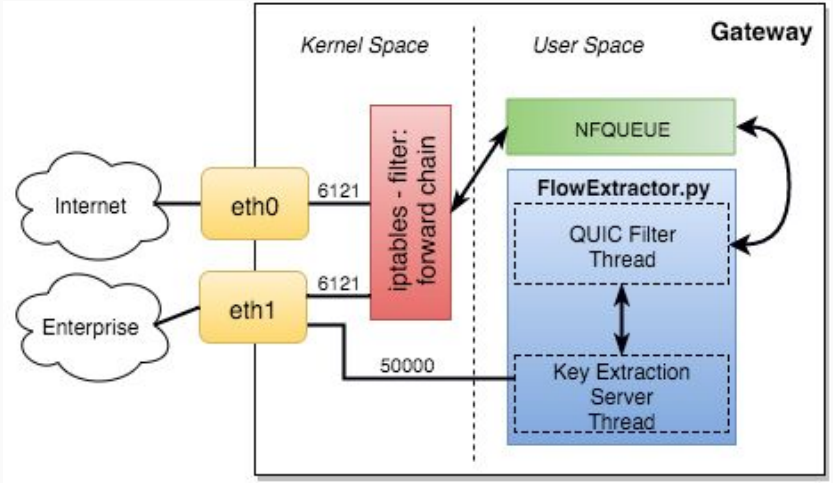
Upgrading QUIC to UbiCrypt on Client

- Goals:
  - Deployability: minimum change to QUIC source code
  - Performance: minimum latency
- Modified QUIC crypto module: write keys to file
- Added external key sharing Python module



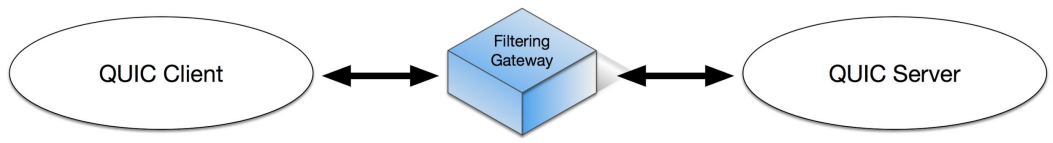
Gateway Architecture

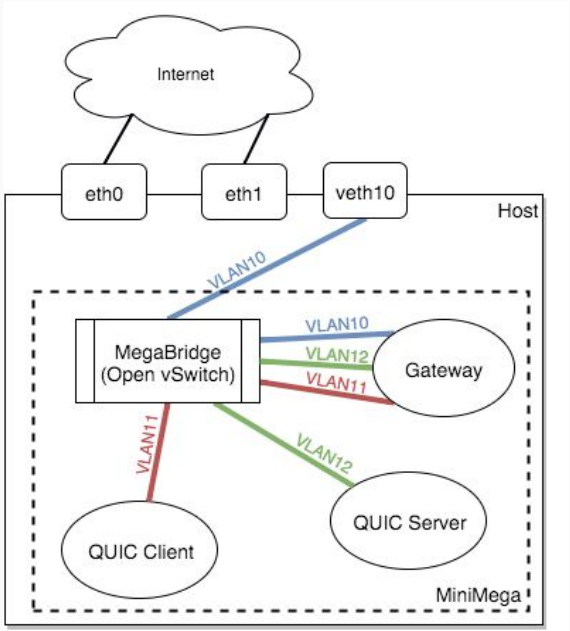
- Two part architecture
  - filtering and forwarding QUIC flows
  - leaked key server
- Filter/Forward
  - iptables for kernel space filtering
  - iptables library extension: NFQUEUE
  - ScaPy for user space processing
  - key-flow matching and management
- Key Server
  - run simple server on port 50000
  - sends leaked keys to filter/forward software



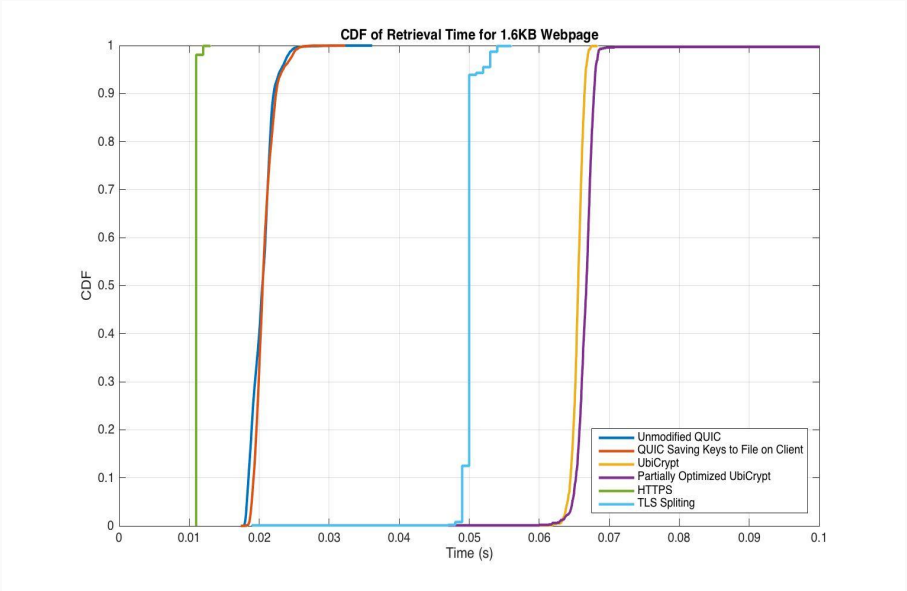
Evaluation

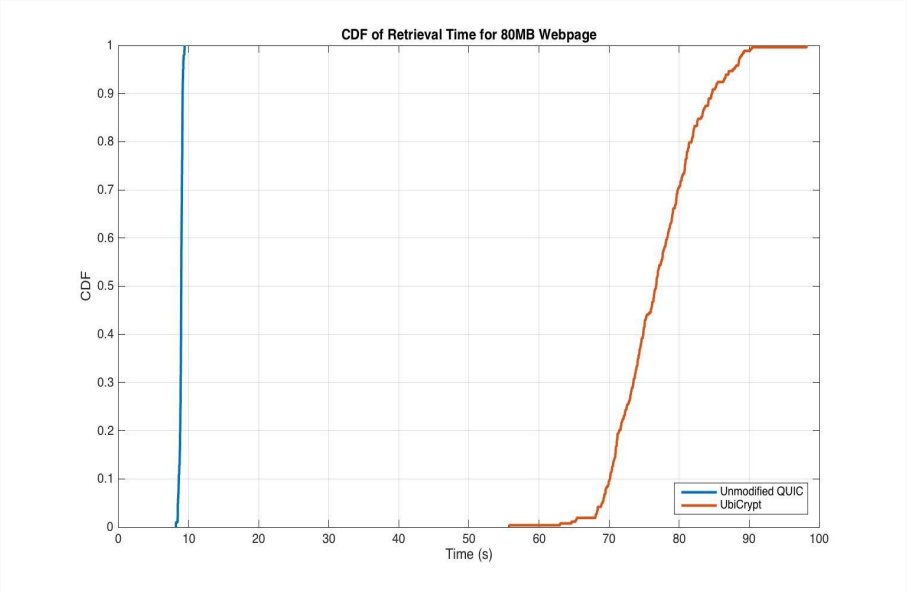
- Built virtual network infrastructure: minimega
- Performance metrics:
  - Latency: small page (1.6KB) retrieval time
  - Throughput: large page (80MB) retrieval time



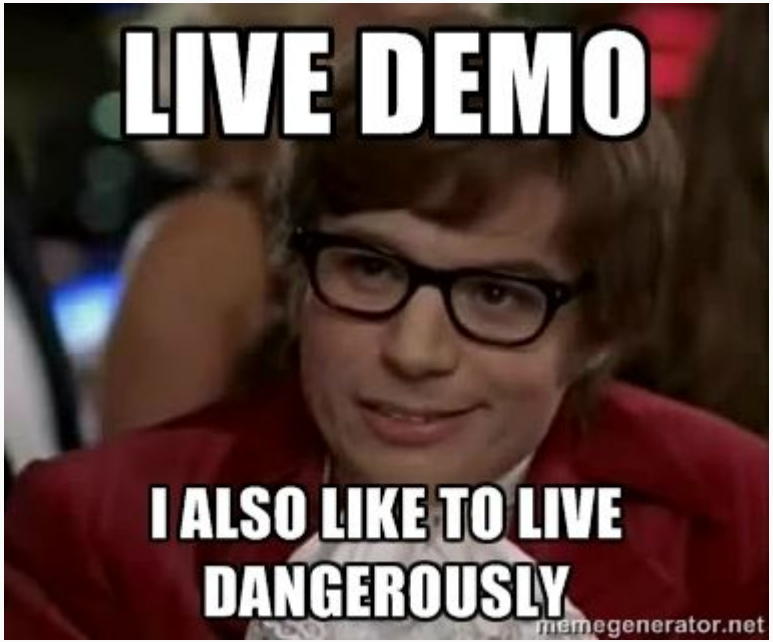


Performance





Demo


LIVE DEMO
I ALSO LIKE TO LIVE DANGEROUSLY
memegenerator.net

Discussion

- Optimization
  - Switching to faster language
  - Moving to kernel
- First packet introspection
  - “Unlock” packet - plaintext of first packet
  - Leak client’s half of ephemeral key

Questions