Protocol Evolution Towards a more Privacy Preserving Internet

Magnus Westerlund
Ericsson Research

Biography

- Works at Ericsson Research in Kista since 2000
  - Worked on real-time media transport and transport protocols
  - Currently focusing on QUIC, MASQUE and 6G Mobile Network Architecture
- Active in IETF since 2000
  - Transport Area Director 2006-2010, 2019-2021
  - Co-authored: 34 RFCs
    - WebRTC (RFC 7941, 8108, 8834, 8853, 8860, 8861, 8872)
    - Zero-checksum for IPv6 (RFC 6935, 6936)
    - Transport Protocol number registry update (RFC 6335)
    - Many more RTP related

Introduction

- Many user privacy improving efforts ongoing
  - Great for the users
  - The need to improve security is real
- My colleagues work in IETF has made us observed many ongoing activities
  - Will provide an overview of the more important
- These activities target improving user Privacy and security
  - They also have implications for the network

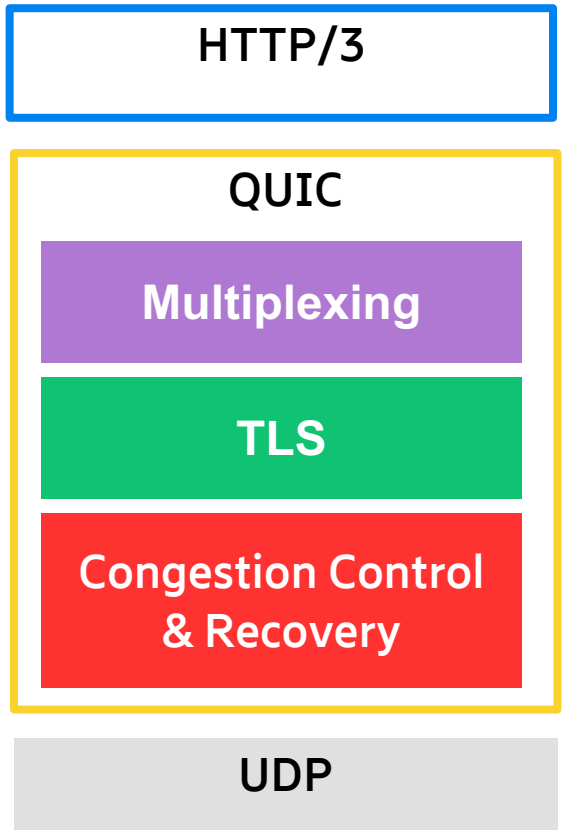
- Traffic classification is significantly challenged by encryption
  - Using machine learning on traffic patterns
  - Continued arms race expected
- We observe some aspects that can affect traffic patterns:
  - Aggregation in tunnel flows
  - Pinning to proxy nodes
- Centralization and Cloudification also plays its role
- Need to find alternatives for management!

QUIC

- QUIC v1 is a fully reliable transport protocol with congestion control
  - TLS 1.3 based security handshake
  - Encrypted and integrity protected payload
  - Protected headers
- QUIC's Wire Image
  - QUIC v1 has one byte unencrypted
  - Rest of Packet header encrypted
- Hard to classify beyond 5-tuple
  - UDP Destination port 443 for HTTP/3
- Implementation specific parameters Transport Extensions will be hidden.

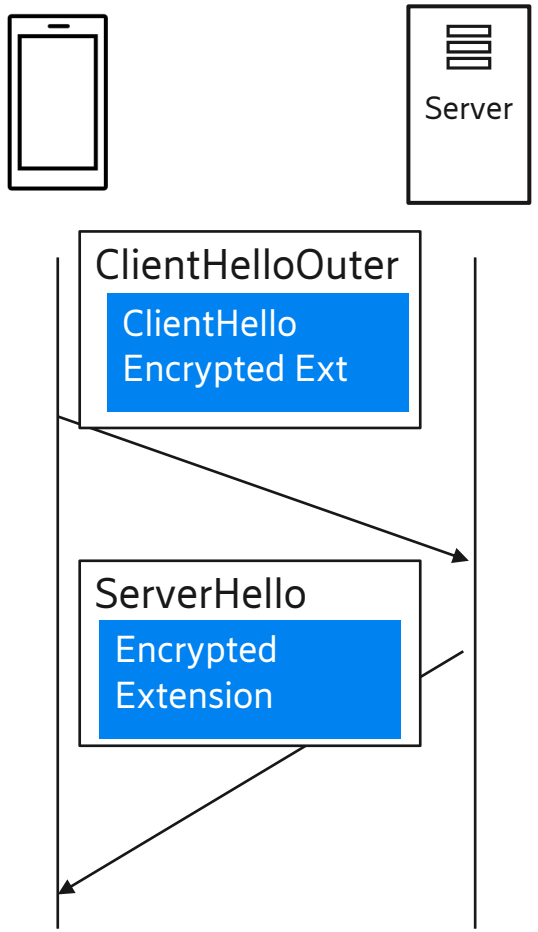
Short Packet form
Header Form (1) = 0,
Fixed Bit (1) = 1,
Spin Bit (1),
Reserved Bits (2),
Key Phase (1),
Packet Number Length (2),

Destination Connection ID (0..160),
Packet Number (8..32),
Packet Payload (8..),
}



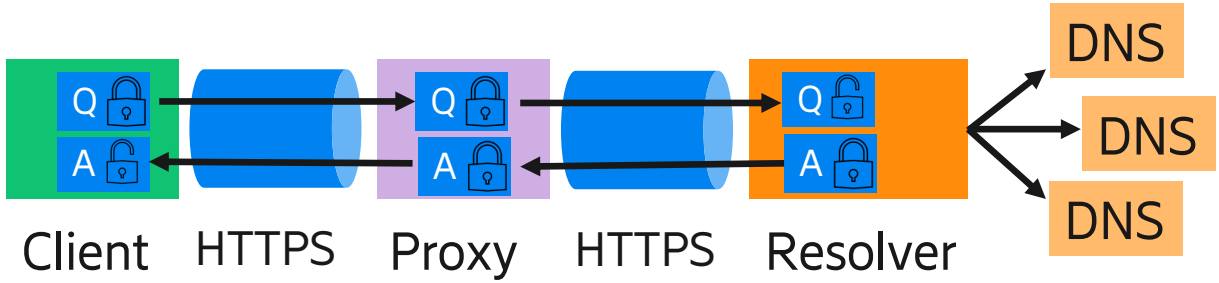
TLS Encrypted Client Hello

- Common to use Server Name Indication (SNI) from the TLS Client Hello to determine which domain a flow is targeting in traffic classification
- TLS Encrypted Client Hello (ECH) puts a stop to this.
  - Client retrieves the ECH provider key using DNS and HTTPS resource records
  - Creates an TLS ClientHelloOuter for the ECH provider and a HPKE protected ClientHello extension with SNI and ALPN etc.
  - If ECH Provider public key was stale, Client Hello outer will result in an error response providing the current public key.



Encrypted DNS

- There are currently a whole set of solutions for secure transport of DNS:
  - DNS over TLS/TCP (DoT)
  - DNS over HTTPS (DoH)
  - DNS over QUIC (DoQ)
- But your resolver will know what you asked and your IP
  - Centralization and usage of e.g. 8.8.8.8 results in concentration of information
  - Oblivious DNS over HTTPS (ODoH) is an answer to separate user id from query
- Traffic capture for resolvers can correlate incoming request and resolver's request

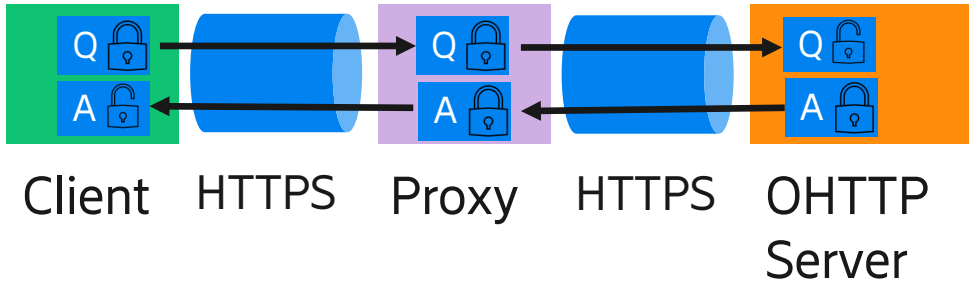


Oblivious DNS over HTTPS

1. Encrypts query (Q) using HPKE with Resolvers key from DNSsec record
2. Sends it to proxy that forwards encrypted query and hides source IP
3. Resolver decrypts and resolves answer (A)
4. Resolver encrypts A with keys from Q and sends to proxy
5. Proxy forwards to client who decrypt A

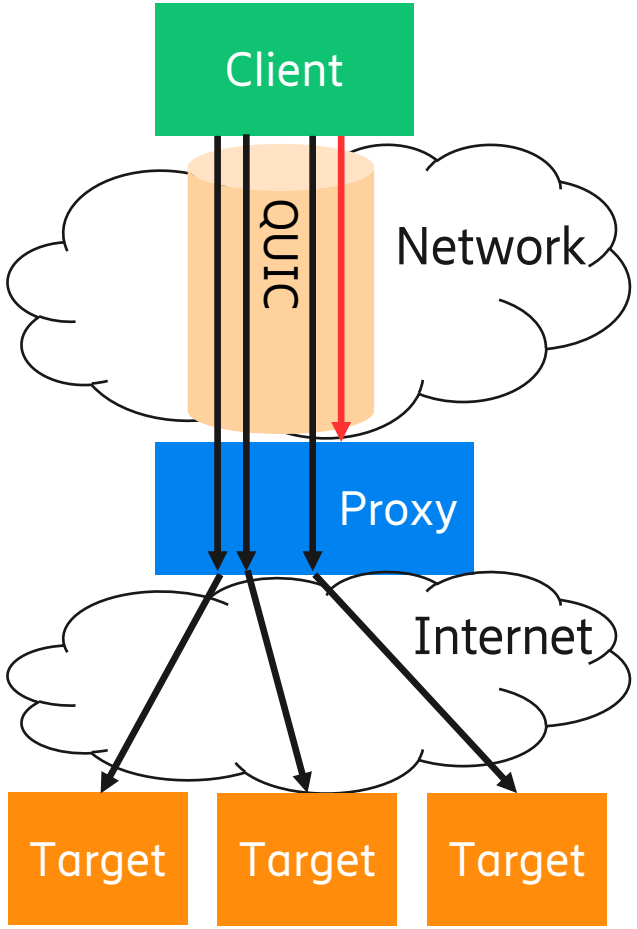
Oblivious HTTP

- Oblivious HTTP is the idea from ODoH but for HTTP
  - HTTP server will not know who requested or posted a resource
  - Proxy does not know the request or post
  - Is not a general replacement for HTTP
    - Request of static resources can work
    - Submission of Telemetry
  - To preserve user privacy, HTTP requests need to be scrubbed from finger printable information



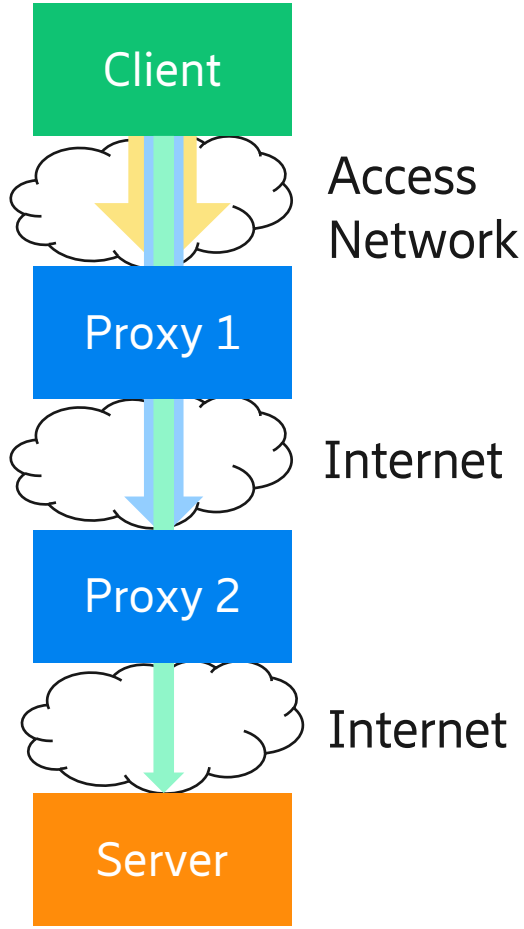
MASQUE and VPNs

- MASQUE is ongoing IETF standardization of tunneling of UDP and IP over QUIC
  - Uses HTTP/3 for control signaling
  - Uses QUIC Datagrams for unreliable, unordered forwarding of E2E packets
  - Multiplexes multiple UDP and IP flows
- Comparable to other VPN tunnels from Privacy perspective
- Implications for Network
  - Tunnel aggregates many flows into single 5-tuple
    - Impacts flow aware Active Queue Management (AQM)
    - Traffic flow logging will only see tunnel flow
  - Pinning the traffic flows to the proxy
    - Affects traffic pattern



Apple's Private Relay

- Private Relay is a privacy preserving proxy relay chain
  - Proxy 1 knows Clients IP
  - Proxy 2 knows Server IP and destination domain
  - Proxy 1 & 2 operated by different entities
- Client <-> Server connection in QUIC tunnel Client <-> Proxy 2
  - Proxy 1 is MASQUE controlled but only rewrites CID and IP/UDP
- Proxy 2 provided with geographical region or Country/Timezone
- DNS over Oblivious DNS but with subnet address for Proxy 1
- Impact
  - Prevents Traffic classification, Content Filtering, Zero Rating
  - Aggregates traffic due to tunneling
  - Pinning traffic to the proxies



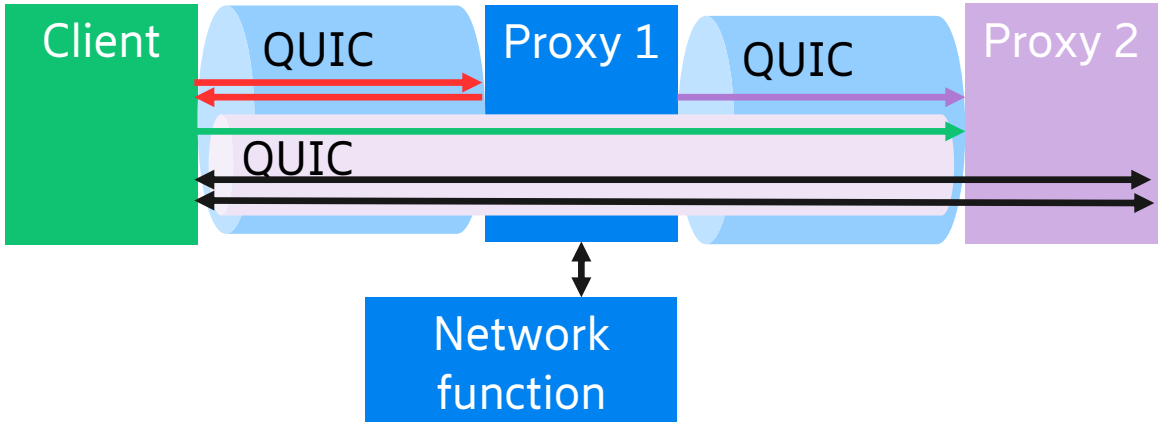
The Future?

- A network operator:
  - Will see large fat flows to a small number of centralized ingresses
  - Little potential for traffic management
- How does network operators meet legal demands on them in relation to carried traffic?
  - The legal demands may have to change
- Service Providers also struggles
  - Where is user?
  - May I provide content to them?

- A Mobile Network view
  - Traffic optimizations to address radio channel are common
    - Lower performance and efficiency
  - Services like zero rating
    - Not possible to offer without collaboration

Explicit Collaboration

- Embrace the possibilities
  - Have Proxy 1 attest client's location to country or region level to Service Provider
  - Make agreements between proxies where Proxy 1 provides zero rating information and proxy 2 reports volumes
  - Send signals to upstream proxy for traffic management
- Explicit Collaboration is beneficial
  - Preserves user privacy better
    - Providing only what is necessary
  - Improves quality of information
    - Enables real trust chains and legal agreements



https://www.ericsson.com/en/blog/2020/6/a-collaborative-approach-to-encrypted-traffic