QUIC-Aware Proxying

draft-pauly-masque-quic-proxy-06

Tommy Pauly, Eric Rosenberg, David Schinazi
MASQUE
IETF 117, July 2023, San Francisco

Agenda

Quick recap

Encryption discussion

Other open issues

Next steps

Recap

Client tells proxy about inner QUIC connection's CIDs (using capsules!)

Proxy may reuse target-facing ports

Client and proxy may skip encapsulation and encryption for proxied SH packets — avoiding cumulative MTU overhead issues

Forwarded mode packets on the wire use virtual CIDs instead of the inner connection's real CIDs

Capsule examples

Client *Proxy*

REGISTER_CLIENT_CID
Connection ID = 0x31323334
Virtual CID = 0x62646668
Stateless Reset Token = Token →

← **ACK_CLIENT_CID**
Connection ID = 0x31323334

REGISTER_TARGET_CID
Connection ID = 0x61626364 →

ACK_TARGET_CID ←
Connection ID = 0x61626364
Virtual CID = 0x123412341234
Stateless Reset Token = Token

CLOSE_TARGET_CID
Connection ID = 0x61626364 →

CLOSE_CLIENT_CID
Connection ID = 0x31323334 →

Open issue

The main question is about encrypting packets in forwarded mode

Forwarded mode swaps CIDs, but not payloads

- This makes correlation packets simple if an observer can see both sides
- Timing and packet size can also make this correlation trivial unless mitigated (padding & timing obfuscation)

Not all threat models require this to be addressed, but it is important for a complete solution

Encrypt all the bytes!

Encryption prevents trivial correlation by passive attackers

- Are we fine scoping the threat model to passive attackers?

AES-CTR approach seems workable

- IV selection
- Single pass vs double pass

AES-CTR proposal

Generate a key and save it next to connection ID

AES-ECB the first 16 bytes

Use those 16 bytes as nonce to AES-CTR the rest of the packet

Many details to be fleshed out: key generation, nonce construction, ...

Should we form a design team?

Open issues

- QUIC Version Compatibility (#83)
- Congestion Control Loops (#81)
- Connection ID Compression (#74)

QUIC Version Compatibility (#83)

- CID registration capsules allow CIDs up to 255 bytes
- Also includes stateless resets which are only defined in RFC9000
- Aligning with QUIC invariants desirable. How should we handle version-specific properties?

Congestion Control Loops (#81)

- Tunneled mode subject to outer-connection's congestion control, while Forwarded mode is not
- Is Forwarded mode worth foregoing the congestion control loop between client and proxy?
  - Seems most relevant when proxy<->target RTT is significant, but this is not always the case.

Connection ID Compression (#74)

- What if you don’t want Forwarded mode, but still want to reduce encapsulation overhead?
- What if CIDs get really large? Cumulative MTU issues become significant.
- Should compression be a separate extension?

Next steps

At 116, the WG seemed in favor of adopting the document and having a design team for encryption

- Let's formally start these, now that MASQUE has rechartered