QUIC-Aware Proxying

draft-pauly-masque-quic-proxy-06

Tommy Pauly, Eric Rosenberg, David Schinazi
MASQUE
IETF 116, March 2023, Yokohama

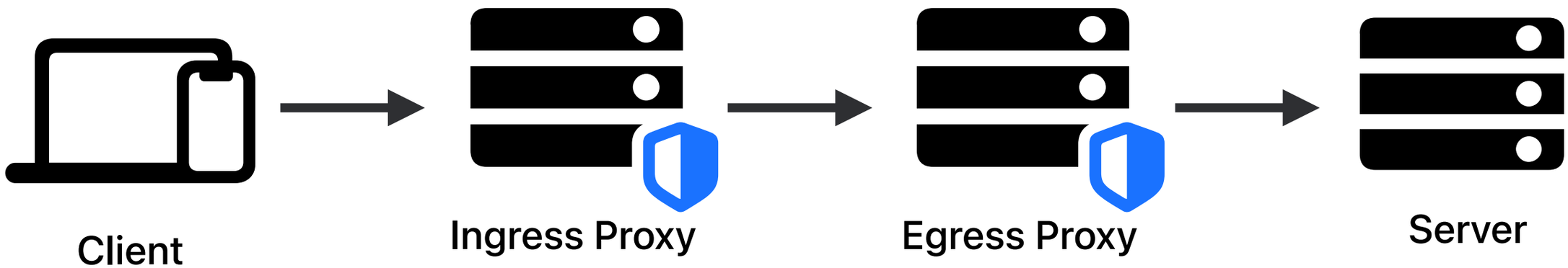
Recap

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


Client
Ingress Proxy
Egress Proxy
Server

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 →

Recent Updates

Virtual connection IDs

- Original versions forwarded end-to-end CIDs

Keepalive behavior for forwarded mode

Migration handling for passive and active migration

ECN behavior

- Forwards markings, can add markings

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

To re-encrypt, or not to re-encrypt?

...and how?

Encryption decisions

Which encryption mechanism?

1. AES-CTR proposal
2. HCTR2
3. Something else?

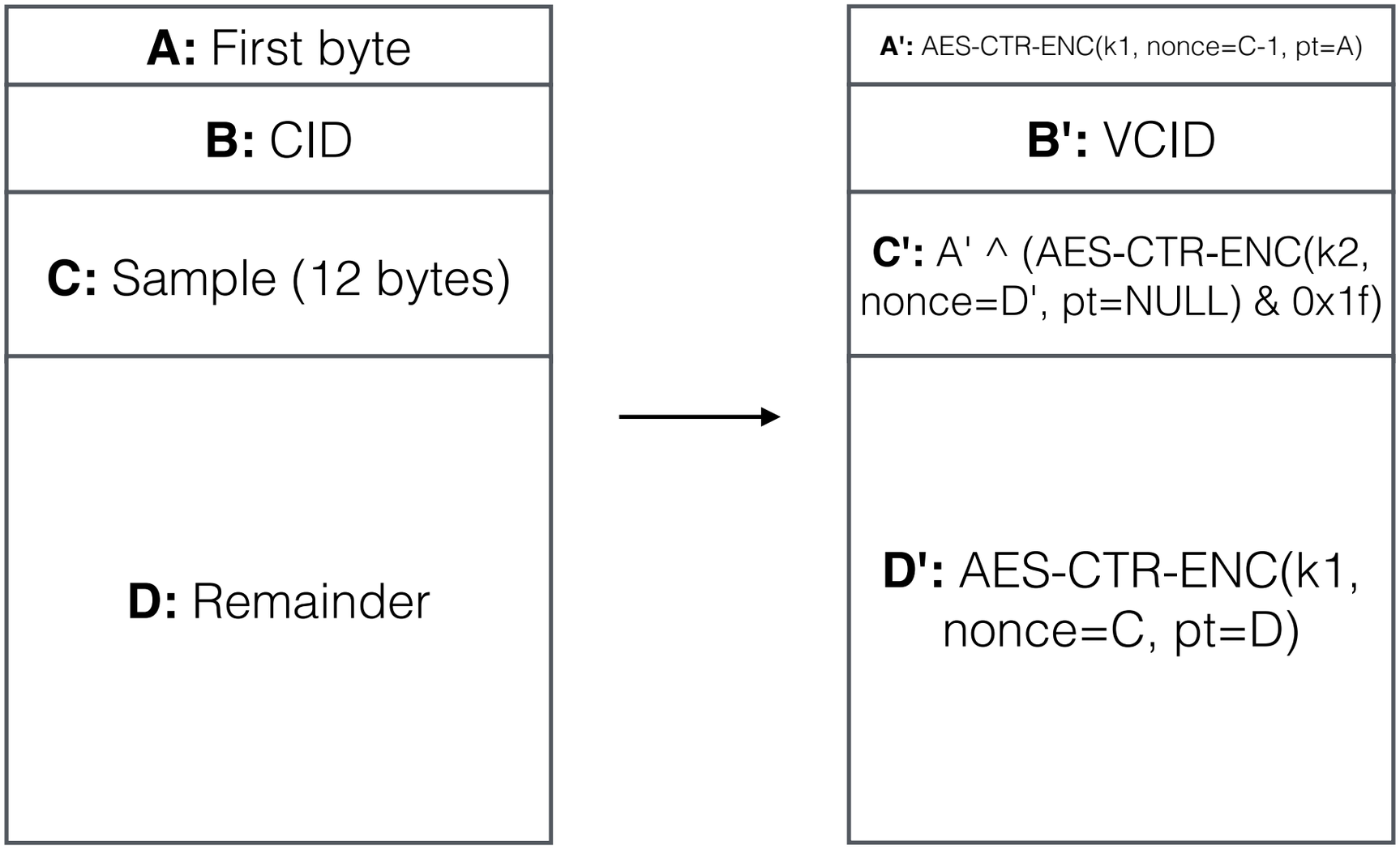
Is re-encryption required?

1. Yes, mandatory for forwarded mode
2. No, negotiated as part of forwarded mode

AES-CTR proposal

Paraphrasing from Martin Thomson

Keys k1 and k2 derived from CID



Question: Does the new first byte look like normal QUIC traffic?

HCTR2

Google authored length-preserving encryption

https://github.com/google/hctr2

https://eprint.iacr.org/2021/1441.pdf

Requires two passes, so likely more expensive

Negotiation

Should forwarding encryption be a negotiable option?

- Use register/ack CID capsules to negotiate
- Choose encryption scheme
- Choose a key

Next steps

Do we want to adopt this document as a starting point?

How should we approach encrypting forwarded packets?

Are there other major features missing?