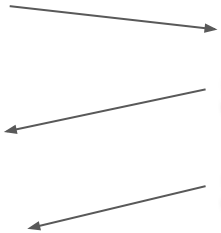
QUIC Version Aliasing

https://datatracker.ietf.org/doc/draft-duke-quic-version-aliasing/

First Connection

Client Initial, version 1



Server Initial, version 1

Server Handshake, TP with:

- random version number (0x433ad370)
- random Initial Token Extension(ITE) (0x19a25b)
- salt (0x453acf30…)
- packet length offset (4233527)

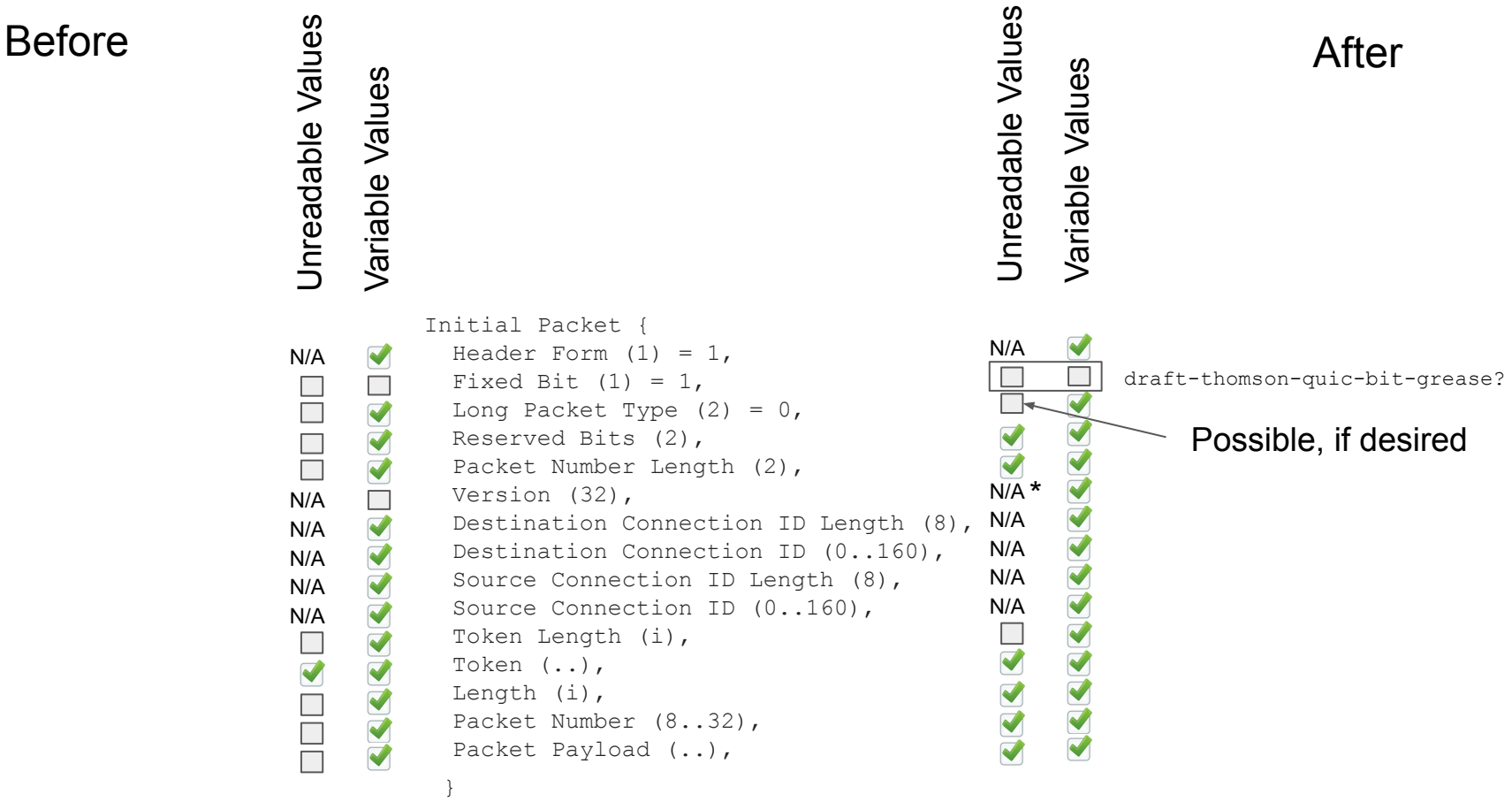
The salt and PLO are a secure hash f(version, ITE)

Next Connection

Client Initial, version 0x433ad370 token {N} + 0x19a25b length = 1200+4233527

Server computes salt from version, ITE

- Connection continues with aliased version number
- Server SHOULD issue TP with new values


Before
Unreadable Values
Variable Values
Initial Packet {
Header Form (1) = 1,
Fixed Bit (1) = 1,
Long Packet Type (2) = 0,
Reserved Bits (2),
Packet Number Length (2),
Version (32),
Destination Connection ID Length (8),
Destination Connection ID (0..160),
Source Connection ID Length (8),
Source Connection ID (0..160),
Token Length (i),
Token (..),
Length (i),
Packet Number (8..32),
Packet Payload (..),
}
N/A
N/A
N/A
N/A
N/A
N/A
N/A
N/A
N/A
N/A *
After
Unreadable Values
Variable Values
draft-thomson-quic-bit-grease?
Possible, if desired

Claimed Properties

- From second connection, Initial packet payloads are **entirely private** and **immune from ossification**
- Minimal TLS ossification vectors over QUIC
- Greases the version field
- Initial Injection attacks are over (maybe VN might work)
- Server has no per-client state
- More space-efficient than ECHO, covers the whole Initial packet, both authenticated and private in both directions
- Does nothing for the first connection
- Dependency on quic-version-negotiation
- Browsers & economically important websites need to deploy it to prevent firewalls from killing it

Potential Improvements: First Connection

- We could declare a v2 where the client provides the salt, encrypted with the server’s ECHO public key from DNS, in the packet header.
- Server extracts this with its private key to get the salt and decrypt the packet

Feedback wanted:

https://github.com/martinduke/quic-version-aliasing

Any browsers and “economically important websites” interested?