QUIC
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2020

Q. An
DP. Liu
YM. Liu
H. Wang
Alibaba Inc.

October 31, 2019

Fast Address Validation
draft-an-fast-address-validation-00

Abstract

This document describes a fast address validation method for QUIC.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 3, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Notational Conventions 2
3. Problem Statement 2
4. Fast Address Validation During Handshake 4
5. Security Considerations 4
6. IANA Considerations 4
7. Normative References 4
Authors' Addresses 5

1. Introduction

As described in [I-D.ietf-quic-transport], a token based scheme is defined to facilitate address validation of a client. The token MUST be covered by integrity protection against modification or falsification by clients. The server remembers the value it sends to clients and validates the token sent back from a client. In its design, Retry packet is used to deliver the token to a client which address has not yet been validated. It voids the first transmission of the Initial packet sent by the client, and triggers a second Initial packet to be sent with the token. The exchange of token will cause unnecessary longer connection establishment delay for a client.

In this document, an alternative mechanism is proposed to improve the efficiency of address validation during handshake. For the first connection between client and server, eliminate the use of Retry packet for token delivery, and rely on handshake encryption layer to prove return routability. In addition, New_Token frame is used by server, via i.e. the Initial packet, to provide the client with an address validation token that can be used to validate future connections.

2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Problem Statement

Address validation is used by QUIC to avoid being used for a traffic amplification attack. In such an attack, a request is sent to a server with spoofed source address information that identifies a victim. If a server generates more or larger packets in response to that request, the attacker can use the server to send more data toward the victim than it would be able to send on its own.

The primary defense against amplification attack is verifying that an endpoint is able to receive packets at the transport address that it claims. Address validation is performed both during connection establishment and during connection migration.

Figure 1 provides an overview of the 0-RTT handshake procedure jointly with address validation defined in [I-D.ietf-quic-transport]. Each line shows a QUIC packet with the packet type and packet number shown first, followed by the frames that are typically contained in those packets. So, for instance the first packet is of type Initial, with packet number 0, and contains a CRYPTO frame carrying the ClientHello.

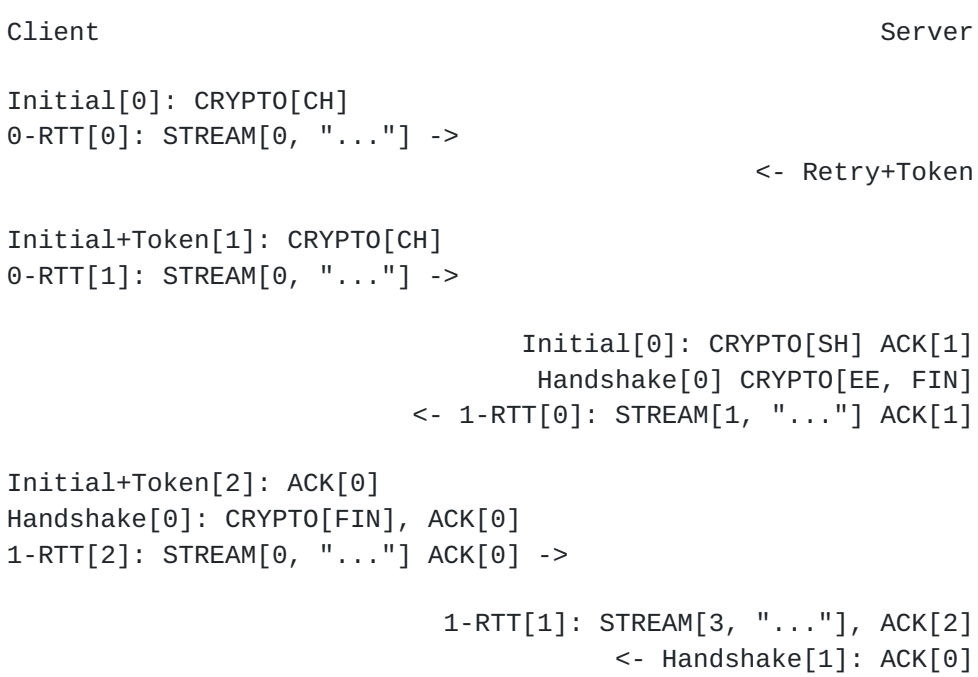

Figure 1: Example of 0-RTT Handshake joint with address validation

Note that, the server acknowledges 0-RTT data at the 1-RTT encryption level, and the client sends 1-RTT packets in the same packet number space.

A server might wish to validate the client address before starting the cryptographic handshake. In [I-D.ietf-quic-transport], a token is defined to provide address validation prior to completing the handshake. Upon receiving the client's Initial packet, the server can request address validation by sending a Retry packet containing a token. When this token is delivered to the client during connection establishment with a Retry packet, the Initial packet has to be re-transmitted from the client including the token. It in turn adds one more round of packet exchange to 0-RTT handshake.

4. Fast Address Validation During Handshake

For the first connection between client and server, server can choose to not use Retry packet for token delivery, but rely on handshake encryption layer to prove return routability. In addition, New_Token frame is used by server, via i.e. the Initial packet, to provide the client with an address validation token that can be used to validate future connections. A flow showing the use of a Handshake packet with the token is depicted in Figure 2.

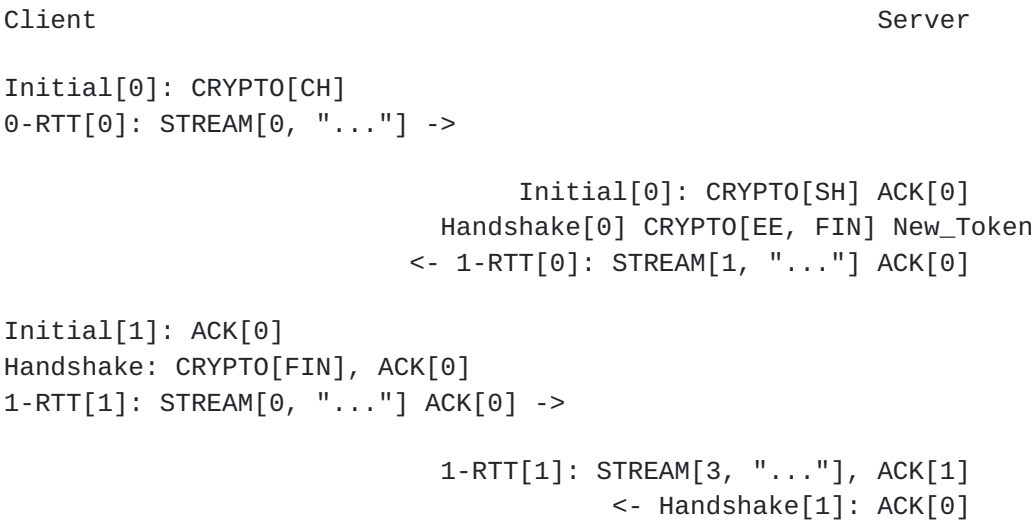

Figure 2: Example Handshake with fast address validation

It is the server's decision whether to exchange token in Retry or just Handshake to validate client address. If server chooses to accept the cost brought by token exchanging in Handshake, due to that server needs to start maintaining handshake states it will bring more enhanced experience in client side.

5. Security Considerations

Adding token field to Handshake packet does not add new security concerns.

6. IANA Considerations

This document makes no request of IANA.

7. Normative References

[I-D.ietf-quic-transport]
Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport", draft-ietf-quic-transport-23 (work in progress), September 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Qing An
Alibaba Inc.

Email: anqing.aq@alibaba-inc.com

Dapeng Liu
Alibaba Inc.

Email: max.ldp@alibaba-inc.com

Yanmei Liu
Alibaba Inc.

Email: miaoji.lym@alibaba-inc.com

Hao Wang
Alibaba Inc.

Email: tars.wh@alibaba-inc.com