Human Rights Protocol Considerations Research Group B. Martini
Internet-Draft Harvard Kennedy School
Intended status: Informational N. ten Oever
Expires: April 25, 2019 University of Amsterdam
October 22, 2018

QUIC Human Rights Review
draft-martini-hrpc-quichr-00

Abstract

QUIC is a new transport protocol that provides low-latency communication and security. QUIC's key features include faster connection establishment, stream-based multiplexing, improved loss recovery, and no head-of-line blocking. This document assesses the potential human rights implications emerging from the deployment of QUIC. The assessment is done based on the methodology articulated in [RFC8280].

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 April 25, 2019.

Copyright Notice

Table of Contents

1. Introduction 3
2. Vocabulary Used 3
3. Review Methodology and Process 5
4. Human Rights Considerations 7
4.1. Connectivity 7
4.1.1. Latency 7
4.1.2. Congestion Control and Loss Recovery 8
4.1.3. Reduced Head-Of-Line Blocking 8
4.1.4. Resources 8
4.2. Privacy 8
4.2.1. Encryption 8
4.2.2. Transparent Proxying 9
4.2.3. Multiple Streams 9
4.2.4. Packet Number Encryption 9
4.2.5. Padding 10
4.2.6. Lawful Intercept 10
4.2.7. Spin Bit 10
4.2.8. Packet Injection 11
4.3. Content Agnosticism 12
4.4. Security 12
4.5. Internationalization 12
4.6. Censorship Resistance 12
4.7. Open Standards 13
4.8. Heterogeneity Support 13
4.9. Anonymity 13
4.10. Pseudonymity 13
4.11. Confidentiality 14
4.12. Integrity 14
4.13. Authenticity 14
4.14. Adaptability 14
4.15. Outcome Transparency 14
4.15.1. Encryption 15
4.15.2. Permissionless Innovation and Its Challenges 15
4.15.3. Privacy, Power and Consolidation 16
4.15.4. Transparency and IoT 17
5. Conclusions and Recommendations 18
6. Acknowledgements 19
7. Security Considerations 19
8. IANA Considerations 19
9. Review Team Information 19
10. References 19
10.1. Informative References 19

10.2. URIs 23
Authors' Addresses 23

1. Introduction

This is a review done within the framework of the Human Rights Review Team, and it was conducted by Beatrice Martini and Niels ten Oever. The Human Rights Review Team aims to implement and improve the guidelines for human rights considerations provided in [RFC8280], and seeks to mitigate potentially adverse human rights impacts that IETF and IRTF documents might have.

Human Rights Reviews are developed by a group of individuals in the IRTF and IETF. They work collaboratively and provide their knowledge and input to the assessments, in an effort to contribute to the IETF open review process. Human Rights Reviews are individual contributions. The authors hope that the comments will be taken into consideration by the draft authors, Working Groups and the IESG.

This review concerns the QUIC protocol in general, and the following drafts in particular: draft-ietf-quic-transport-12, draft-ietf-quic-tls-12, draft-ietf-quic-invariants-01.

2. Vocabulary Used

Anonymity The condition of an identity being unknown or concealed [RFC4949].

Censorship Technical mechanisms, including both blocking and filtering, that state or private actors can use to block or degrade Internet traffic. For further details on the various elements of Internet censorship, see [Halletal].

Censorship resistance Methods and measures to mitigate Internet censorship.

Confidentiality The property that data is not disclosed to system entities unless they have been authorized to know the data [RFC4949].

Connectivity The extent to which a device or network is able to reach other devices or networks to exchange data. The Internet is the tool for providing global connectivity [RFC1958]. Different types of connectivity are further specified in [RFC4084].

Content agnosticism Treating network traffic identically regardless of content.

Heterogeneity "The Internet is characterized by heterogeneity on many levels: devices and nodes, router scheduling algorithms and queue management mechanisms, routing protocols, levels of multiplexing, protocol versions and implementations, underlying link layers (e.g., point-to-point, multi-access links, wireless, FDDI, etc.), in the traffic mix and in the levels of congestion at different times and places. Moreover, as the Internet is composed of autonomous organizations and Internet service providers, each with their own separate policy concerns, there is a large heterogeneity of administrative domains and pricing structures." [FIArch]

As a result, per [FIArch], the heterogeneity principle proposed in [RFC1958] needs to be supported by design.

Human rights Principles and norms that are indivisible, interrelated, inalienable, universal, and mutually reinforcing. Human rights have been codified in national and international bodies of law. The Universal Declaration of Human Rights [UDHR] is the most well-known document in the history of human rights. The aspirations from [UDHR] were later codified into treaties such as the International Covenant on Civil and Political Rights [ICCPR] and the International Covenant on Economic, Social and Cultural Rights [ICESCR], after which signatory countries were required to reflect them in their national bodies of law. It is also broadly recognized that not only states, but also non-state actors must respect human rights.

Integrity The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner [RFC4949].

Linkability Establishing the identity of a host across several IP addresses.

Open standards As stated in [RFC2026]: "Various national and international standards bodies, such as ANSI, ISO, IEEE, and ITU-T, develop a variety of protocol and service specifications that are similar to Technical Specifications defined here. National and international groups also publish "implementors' agreements" that are analogous to Applicability Statements, capturing a body of implementation-specific detail concerned with the practical application of their standards. All of these are considered to be 'open external standards' for the purposes of the Internet Standards Process."

Openness Absence of centralized points of control - "a feature that is assumed to make it easy for new users to join and new uses to unfold" [Ziewitzetal].

Ossification The increasing inflexibility of the network which results in the inability to deploy a new protocol or protocol extensions due to the unchangeable nature of infrastructure components that have come to rely on particular features of current protocols.

Permissionless innovation The freedom and ability to freely create and deploy new protocols on top of the communications constructs that currently exist.

Privacy The right of an entity (usually an individual), acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others [RFC4949].

The right of individuals to control or influence what information related to them may be collected and stored, and by whom and to whom that information may be disclosed.

Privacy is a broad concept regarding the protection of individual or group autonomy and the relation between an individual or group and society, including government, companies, and private individuals. It encompasses a wide range of rights, including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. It is commonly recognized as a core right that underpins human dignity and other values such as freedom of association and freedom of speech. The right to privacy is also recognized in nearly every national constitution and in most international human rights treaties. The right to privacy is also legally protected at the national level through provisions in civil and/or criminal codes.

Pseudonymity The ability to use a persistent identifier that is not immediately linked to an individual's offline identity. Pseudonymity is an critical feature for many end users, as it allows them different degrees of disguised identity and privacy online. "Pseudonymity is strengthened when less personal data can be linked to the pseudonym; when the same pseudonym is used less often and across fewer contexts; and when independently chosen pseudonyms are more frequently used for new actions (making them, from an observer's or attacker's perspective, unlinkable)." [RFC6973]

3. Review Methodology and Process

This section describes how the review was undertaken.

We started our review by examining the Internet Drafts which were active on June 7, 2018 on the QUIC Working Group Datatracker (https://datatracker.ietf.org/wg/quic/documents).

Inferential reading of the documents resulted in the decision to focus our efforts on three specific drafts: draft-ietf-quic-transport-12, draft-ietf-quic-tls-12, draft-ietf-quic-invariants-01.

From the study of these documents through the perspective of the Guidelines for Human Rights Protocol Considerations outlined in [RFC8280], we formulated a questionnaire, to be used as a tool to guide semi-structured interviews with QUIC Working Group chairs and document authors.

We engaged in a total of seven interviews, which took place during IETF102 (July 14-20, 2018). These were then transcribed and analyzed. The analysis focused on the identification of potential positive or negative impacts on human rights, and on the categorization of our findings according to the Guidelines for Human Rights Protocol Considerations outlined in [RFC8280].

One particular aspect that is critical to consider is the pace at which the QUIC Working Group operates, which is regarded across the IETF community as notably faster than usual. This means that while the general design that is outlined in the QUIC Internet Drafts is fairly stable, numerous details are in constant change. When it comes to conducting an interview-based research, this also means that some of the expressed points of view might be overtaken by intervening changes. To address this specific characteristic of the work on the QUIC protocol, we decided to set a time point to examine active Internet Drafts and current Working Group discussions. The time point is June 7, 2018. In addition to that, we also kept discussing with the interviewees, reviewing notes from the following New York interim meeting (September 19-20), and following selected mailing list threads, until our final review of this very document, on October 17, 2018.

The content examined until the set time point (June 7, 2018) is what should be considered the core subject of our examination. However, as we aim to helpfully contribute to the efforts of the QUIC Working Group, we also decided to monitor potential updates and emerging discussions which took place in the following months, with the aim to provide relevant and applicable feedback.

4. Human Rights Considerations

The Human Rights Protocols Considerations Research Group (HRPC) welcomes the drafts draft-ietf-quic-transport, draft-ietf-quic-tls, draft-ietf-quic-invariants.

In particular, we welcome the efforts to improve connectivity on high latency, low bandwidth and high loss connections, and the application of encryption by default. Conclusions and recommendations can be found at the end of this document.

No implications for Accessibility ([RFC8280], sec. 6.2.11), Localization ([RFC8280], sec. 6.2.12), Decentralization ([RFC8280], sec. 6.2.13), and Reliability ([RFC8280], sec 6.2.14) have been found.

4.1. Connectivity

Overall, QUIC is expected to result in a greatly improved Internet service for users worldwide, and in particular for those who currently do not have high bandwidth or lossless connections. Regions that currently do not benefit from reliable connectivity, would be provided with a significantly improved service. These advancements have positive implications in regards to human rights such as freedom of expression, freedom of association, right to political participation.

4.1.1. Latency

QUIC was designed as a new transport protocol to provide connections with lower latency than previous protocols.

One of the most important differences between TCP and QUIC connections is that QUIC connection establishment takes 0 RTTs when a server is known by a client and up to a few RTTs for the first connection to an unknown server.

By allowing for Zero-Round Trip Time (0-RTT) resumption of connections, QUIC performs better than TCP on high latency and high loss connections. When a web client uses TCP and TLS, it requires two to three round trips with a server to establish a secure connection before the browser can send a request. With QUIC, if a client has communicated with a server before (within a specific time period), it can start sending data without any round trips, so that web pages will load faster.

An example of QUIC's performance can be observed on a well-optimized site like Google Search, where connections are often pre-established,

and QUIC's faster connections can only speed up some requests. Still, QUIC improves mean page load time by 8% globally, and up to 13% in regions where latency is higher. [Behretal]

4.1.2. Congestion Control and Loss Recovery

QUIC's congestion control is based on TCP NewReno [RFC6582], a congestion window based congestion control. The signals QUIC provides for congestion control are generic and are designed to support different algorithms. In this way, QUIC can be configured to fit best in different contexts.

Compared to TCP, QUIC offers more detailed feedback information for loss detection. For example, it uses a monotonically increasing packet number and does not retransmit on the packet-level but on the content-level. This allows QUIC to distinguish retransmissions from the originally sent packets, avoiding retransmission ambiguities.

Overall, comparing it to previously existing protocols, QUIC implements better estimation of connection RTTs and detects and recovers from loss more efficiently.

4.1.3. Reduced Head-Of-Line Blocking

HTTP/2 allows multiple objects to be fetched over the same connection, using multiple streams within a single flow.

In TCP, if a loss occurs in one stream, all streams stall while waiting for packet recovery. Differently, QUIC allows other streams to continue to exchange packets even if one stream is blocked due to a missing packet [MolaviKakhkietal].

4.1.4. Resources

QUIC is relatively expensive to implement, both in terms of code (size and complexity) and processing (including memory overheads). This can represent a barrier to adoption and the benefits that come with that.

4.2. Privacy

4.2.1. Encryption

QUIC incorporates the key negotiation features of TLS 1.3, requiring all connections to be encrypted.

Encryption improves the security and privacy of user data. It is built into QUIC, using AEAD algorithms such as AES-GCM and ChaCha20

for both privacy and integrity. QUIC authenticates the parts of its headers that it does not encrypt, so attackers cannot modify any part of a message [Behretal].

Furthermore, in addition to improving privacy, encryption helps to address the ossification of network protocols caused by middleboxes that assume certain information to be present in the clear [Kuehlewindetal].

4.2.2. Transparent Proxying

Many cellular and high-latency networks use transparent TCP proxies to reduce end-to-end delays and improve loss recovery. However, by encrypting the transport headers, QUIC prevents transparent proxying, thus protecting their integrity [MolaviKakhkietal].

4.2.3. Multiple Streams

By establishing connection with multiple streams, QUIC creates higher opacity for the observer.

Comparing QUIC to TLS over TCP, QUIC significantly reduces the amount of information that an observer can acquire about communications they are looking at.

In TCP, all of the information regarding the protocol flow at a transport layer is exposed, and can be used to identify active communications.

In QUIC, it is possible to have an established connection with an end point and to run multiple streams over that connection. Consequently, an observer who is looking at someone's connection, would not be able to tell the difference between the streams.

4.2.4. Packet Number Encryption

In QUIC packet numbers are encrypted.

From a general standpoint, the number assigned to each packet carries very little information. For example, it is possible to observe that a packet sent a certain time and the packet that was sent immediately after probably have increasing packet numbers.

But when traffic is carried over multiple paths, it becomes observable at many points, and this has privacy implications. For example, as stated in [draft-huitema-quic-mpath-req-01]: "[...] if packets belonging to a given connection carry some unique identifiers, observers could use these identifiers to track client

migrations through several paths, and thus potentially expose the successive locations of a particular user."

4.2.5. Padding

Bit padding is the addition of one or more extra bits to a transmission or storage unit to make it conform to a standard size.

QUIC (like HTTP/2 and TLS) offers a padding mechanism that can be used as a defense against traffic analysis for protected packets. It is important to note that its use is discretionary by implementations.

4.2.6. Lawful Intercept

The lawful intercept of content in QUIC works similarly to TLS over TCP. An intercept can: force the acceptance of an alternate certificate; cooperate with or coerce the non-monitored endpoints to obtain session keys for decryption of traffic; exploit endpoint vulnerabilities to place monitoring devices directly on the endpoint on the other side of the crypto boundary.

Forcing TLS 1.3 avoids some common exploit vectors in TLS 1.2 and strengthens the ciphersuites.

4.2.7. Spin Bit

When Google offered the IETF the opportunity to take the work on QUIC and produce an open standard that could be used by all [Wilketal], it sparked off a debate within the IETF as to how much transport information should be deliberately kept unknown to the network.

As an explicit design goal, QUIC provides far less information about its operation to devices on path than TCP does. In TCP, the sequence and acknowledgement numbers and timestamps (if the respective option is in use) can be seen by on-path observers, and used to estimate end-to-end latency.

Differently from previous transport protocols, QUIC splits the information it uses for its own operation from its wire image. As a consequence, QUIC's wire image currently does not expose any information that can be used for passive latency measurement techniques [draft-ietf-quic-spin-exp-00].

At the June 2017 interim meeting of the QUIC Working Group, a proposal was made to add a latency spin bit to QUIC's wire image, in order to allow for passive measurability of RTT equivalent to TCP [Trammell01].

The spin bit is an explicit signal for passive measurability of round-trip time. It causes one bit in the header to 'spin', generating one edge (a transition from 0 to 1 or from 1 to 0) once per end-to-end RTT.

During the following months, the proposal to add this facility to the QUIC protocol has been further discussed and researched. At IETF101 the Working Group agreed upon the reservation of three bits for experimentation with passive RTT measurement, with the result of this experimentation to inform an eventual working group decision whether to include the bit in the shipping version 1 of the protocol, scheduled to be complete by November 2018. [Trammell02]

From its designers' perspective, the spin bit was formulated to be a minimal-risk, maximum-utility signal fit for a single purpose: on-path measurement of end-to-end RTT, to generate RTT samples for a variety of passive latency measurement tasks.

The key argument in favor of the spin bit originates from the notion that measurement is fundamental to the operation of networks and at-scale services, whether for management, security, optimization, and that if it is at all possible to safely design passive measurability of any metric explicitly into a protocol, this signal represents how to do it. [Trammell01]

The argument made by those who are not in favor of the addition of the spin bit to the protocol, is that the exposure of any information beyond the IP header and the base essentials of a UDP header is not necessary and not safe. They point out that how this bit may be used, were it to be added to the protocol, is unknown.

This could represent an infringement of the user privacy. Furthermore, an exposed bit might cause for ossification of the bit itself, which would, to some extent, defeat QUIC's efforts to elude the intrusive and ossifying grip of network middleware. [Huston]

4.2.8. Packet Injection

It is viable for network operators to add data to packets in order to do traffic monitoring and/or management. It is not uncommon for network operators to routinely tag packets as they enter the network for their own purposes, and simply erase the tag when they leave the network. Packet modification or injection cannot be prevented in QUIC. However, the protocol takes steps to ensure that its own state is not affected by this kind of activity.

4.3. Content Agnosticism

The QUIC protocol itself is content agnostic. While it is currently being optimized for HTTP traffic, it can also be used with other application layer protocols (e.g. see [draft-huitema-quic-dnsoquic-05]).

4.4. Security

QUIC improves security by making encryption an inherent part of the transport protocol, instead of adding it as a optional layer on top of it. This protects the integrity of the data by preventing tampering on the path, and ensures end-to-end confidentiality between the two communicating hosts. Furthermore, it ensure that no on-path party can emulate an endpoint.

By encrypting all Internet traffic by default it is harder for researchers and network operators to analyze network traffic. This is a specific design goal, but it also makes research into the promulgation of malware, cookies and other artefacts much harder, since in this case access to the stream needs to be provided by the end point.

4.5. Internationalization

[draft-ietf-quic-transport-12] does not define human readable strings, except for where it states that the Reason Phrase in the CONNECTION_CLOSE and APPLICATION_CLOSE frames "SHOULD be a UTF-8 encoded string [RFC3629]". The QUIC protocol demands that this SHOULD be an UTF-8 string, while UTF-8 is actually not required. Also, there is currently no space to declare the charset used. So it is recommended that this SHOULD becomes a MUST.

[draft-ietf-quic-transport-12] does not allow for the use of language tags. If it would request these tags, it would allow implementations to signal in which language Reason Phrases are rendered.

4.6. Censorship Resistance

Encryption makes monitoring and filtering of the traffic more complex, thus hindering fine-grained censorship.

Furthermore, in QUIC it is also harder to terminate connections, since in the protocol the only parties that can terminate the connection are those actually involved in the connection once it exists. This means that a middlebox cannot reset a connection, but needs to continue to block it, keeping state. Considering this, it

can be stated that QUIC makes censorship harder because it requires the censor to invest more resources and efforts.

QUIC is also improving the protection against DDoS through observation of the handshake for connection confirmation, and through the need to validate new connections in case of a connection migration.

It is worth noting that it is almost impossible to make the handshake resilient to injection attacks, and the general consensus has been not to spend cycles trying. This means that handshakes can easily be disrupted by a censor. Post-handshake, QUIC is very resilient to attempts to reset the connection by a third party.

4.7. Open Standards

QUIC is published as open standard.

4.8. Heterogeneity Support

The design of the QUIC transport protocol is currently specifically tailored to be used with TLS1.3 and HTTP2. It is explicitly constructed in a modular manner and is designed to support other application layer protocols in the future as well.

4.9. Anonymity

Persistent static identifiers, consistently linking to a particular person or small, well-defined group of people, are one of the main threats to anonymity. This is especially concerning when the identifier is used in repeatedly used in multiple contexts, thus raising an issue of linkability.

In QUIC, linkability would occur in case a connection ID was used on multiple network paths. In order to provide some protection against linkability in case of connection migration, QUIC uses different connection IDs when different local addresses are used. Furthermore, packet numbers are encrypted to ensure they are not used to establish a link between different connection IDs.

However, it is important to note that traffic analysis might still allow to correlate different streams.

4.10. Pseudonymity

Keeping different identities isolated from each other is critical to protect and preserve pseudonymity. QUIC contributes to this by using different connections IDs for different local addresses.

4.11. Confidentiality

Through the use of cryptography, QUIC integrates security, confidentiality, authenticity, and integrity directly into the transport protocol rather than having them layered on top of it. Any server that offers QUIC to benefit from its latency improvements will automatically provide all the aforementioned attributes to their user.

4.12. Integrity

The use of TLS1.3 in QUIC makes on-path attacks either visible or nearly impossible to carry out. So, if an actor forces the traffic to go through one middlebox and decrypt the traffic itself, their action is made detectable. This also protects the integrity of the datastream, prevents tampering, and averts the injection of extra data in the stream.

4.13. Authenticity

Except for the initial handshake, the encryption in QUIC is provided by TLS1.3, which uses asymmetric cryptography to authenticate the hosts. This enables verification of authenticity.

4.14. Adaptability

QUIC has a modular approach, and is designed for adaptation. The only commitments in the protocol are the requirement to run on UDP, the packet header, and the version negotiation phase. The remainder of the protocol is quite flexible and can be further adapted.

By preventing the ossification of the protocol by middleboxes through the encryption of transport headers, QUIC enhances the adaptability of the architecture.

As a transport protocol, QUIC tries to be agnostic for application layer protocols, even though it is currently tailored to work with HTTP/2.

4.15. Outcome Transparency

Outcome transparency concerns the intelligibility of the effects of a protocol in relation to its users, protocol developers, and implementers, and its potential consequences (e.g. lack of authenticity may lead to lack of integrity and negative externalities)[RFC8280].

QUIC represents a remarkable evolution of the transport layer with significant impact on the Internet architecture and, most importantly, the service provided to users.

4.15.1. Encryption

The IETF has reached consensus on the fact that pervasive monitoring is an attack (see [RFC7258]), and that a response to mitigate this is represented by ubiquitous encryption, which would also reinforce the end-to-end nature of the network [RFC2775] [RFC3724] [RFC7754].

With the advent of QUIC, encryption becomes the default on the transport level. This has a critical impact on the protection of user privacy.

Furthermore, it has implications concerning network operators that had previously used visible parts of protocols to, among other things, manage, operate, and secure their networks [RFC8404].

Encryption also improves the integrity of the datastream, as QUIC allows to protect users against injections of ads by network operators.

4.15.2. Permissionless Innovation and Its Challenges

As suggested by interviewees during the research phase of this review, and to acquire a more contextualized understanding of protocol development efforts over time, it is relevant to pay attention to the history of SCTP (Stream Control Transmission Protocol). SCTP is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network, standardized in [RFC4960].

As outlined in the comparison between SCTP and QUIC presented in [draft-joseph-quic-comparison-quic-sctp-00], the deployment of SCTP is not particularly widespread. In-network devices, like NAT gateways for example, do not support SCTP well. NAT gateways need to be upgraded to be SCTP-aware, the modification of middleboxes is very expensive, and Internet service providers, focusing on the sustainability of their business, update the devices in accordance with the benefit that this can represent for their revenues.

Furthermore, an early version of QUIC (now popularly called gQUIC) was initially designed and deployed by a large content provider, Google. It was implemented in 2012, and the company invested significant resources to develop it, for example conducting thorough A/B-testing in order to assess how the protocol would interact with

the network, and how the middleboxes would respond. QUIC is now widely used in Chrome clients accessing Google services.

In 2015, an Internet Draft of a specification for QUIC was submitted to the IETF for standardization, and the following year the QUIC Working Group was established. A growing number of contributors from the corporate, academic, nonprofit sector have joined the protocol development work since, and what has been achieved to date is the result of a notable and labor-intensive collaborative effort.

So, on one hand, the history of QUIC shows that permissionless innovation is still possible. On the other hand, it also shows what remarkable efforts and resources are needed to carry out such an ambitious project. While permissionless innovation still exists, the threshold and costs for innovation seem to rise significantly and increasingly.

Also, a look at the actors and dynamics involved in QUIC's history should not underestimate the power of Google's authority. A different developing actor might have been able to invest a similar amount of resources into the development of a protocol. Still, without an impressive user base and traffic stream as Google's, they might have received a less supportive response from network operators.

Having said that, it is expected that QUIC will improve the current situation by providing a more capable transport which aims to overcome ossification and allow for changes in the protocol due to its modularity.

4.15.3. Privacy, Power and Consolidation

The most relevant privacy advantage provided by QUIC is gained by users who have different kinds of traffic relations with one end point. In fact, QUIC does not allow network providers to easily differentiate between, for instance, HTTP requests, DNS requests and real time voice packets, thus strengthening user privacy, and also improving performance. It is important to note, though, that QUIC does not actually hide or attempt to hide the application protocol being used on a connection. The ALPN offered by the client is protected only by a key which can be calculated by any party who can work with the QUIC version in use.

On the other hand, this creates a concentration of different kinds of traffic with one end point, thus giving the service provider access to more categories of privacy sensitive information.

In the current reality of the Internet, the biggest hosts are controlled by large, consolidated, transnational corporations. This creates an extreme power differential between end users on the one hand, and service providers and content operators on the other hand.

In order to protect privacy and secure information, it is important that the user makes a careful and informed decision about the hosting provider and plan they choose.

While ubiquitous encryption changes the relation between service providers and content operators, placing them at the same end of the spectrum, it remains to be seen whether if it can help users take and retain control within the overall power structures of Internet governance and economics.

One of the problems with deploying fully encrypted protocols like QUIC is that deployment is far easier for organizations that already have integrated observability, traceability, and tooling in their back-ends, which not surprisingly happen to be the big players.

If there was any chance to make running a QUIC server relatively easy, thus enabling a greater diversification of end points, QUIC could contribute to a power shift in favor of the end user.

However, running a QUIC infrastructure is currently expected to be more demanding than running a HTTP/2 or HTTP/1 infrastructure. It would be truly compelling if this consideration could be discussed further, and ideally addressed by the development and release of openly available tooling allowing for more accessible ways to run a QUIC server.

4.15.4. Transparency and IoT

End-to-end encryption on the transport layer makes monitoring and filtering of the traffic more complex, and can lead to the adoption of other network management practices to obtain this information.

This has implications on the management of Internet of Things (IoT) devices. If an IoT device adopts QUIC, it will be harder for the user who owns the device to monitor what data is communicated with third parties. It would also be more difficult to conduct research into the promulgation of malware, cookies and other artefacts.

Adequate tooling to protect the right to privacy of IoT users has not yet been developed.

5. Conclusions and Recommendations

The QUIC protocol provides significant human rights improvements for end users.

It dramatically improves connectivity for users on high-loss, high-latency connections. Users will benefit from lower latencies and will not need to restart sessions as often. And in those cases in which they will need to restart a session, they will able to do so without having to re-do the initial handshake.

Another key improvement is represented by the use of encryption by default, which provides authentication, stream integrity, adaptability of the protocol by overcoming ossification, and improved protection from third party monitoring and metadata analysis.

The following is a list of potential improvements that we invite the QUIC Working group to take into consideration, wishing for the protocol to have even greater positive implications for human rights.

- As the QUIC Working Group is expected to deliberate on the potential inclusion of the spin bit in the main specification of the protocol at the upcoming IETF103 (November 3-9, 2018), we suggest to consider not to include it. Our recommendation is motivated by the concerns raised in regards to its implications on user privacy, as reported in this very document, and also shared by some of the interviewees.

- Consider deploying IP header encryption as an optional extension.

- Evaluate the addition of language tagging and charset identification in the case of Reason Phrase in the CONNECTION_CLOSE and APPLICATION_CLOSE.

- Examine the opportunity to translate the QUIC specification into other languages.

- Discuss the viability to make tooling for running QUIC servers openly available.

- Observe and iteratively assess the implications of QUIC on the power relations between end user on one end of the spectrum, and network operators and service providers on the other one.

6. Acknowledgements

The authors thank (in alphabetical order) Mike Bishop, Janardhan Iyengar, Daniel Kahn Gillmor, Mirja Kuehlewind, Mark Nottingham, Martin Thomson, and Brian Trammell for their generous contribution to our research and review. This document does not necessarily reflect their opinion, but solely that of the authors.

7. Security Considerations

As this draft concerns a research document, there are no security considerations.

8. IANA Considerations

This document has no actions for IANA.

9. Review Team Information

The discussion list for the Human Rights Review Team is located at the e-mail address hr-rt@irtf.org [1]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hr-rt [2]

Archives of the list can be found at: https://www.irtf.org/mail-archive/web/hr-rt/current/index.html [3]

10. References

10.1. Informative References

[Behretal] Behr, M. and I. Swett, "Introducing QUIC Support for HTTPS Load Balancing", June 2018, <https://cloudplatform.googleblog.com/2018/06/Introducing-QUIC-support-for-HTTPS-load-balancing.html>.

[Cuietal] Cui, Y., Li, T., Liu, C., Wang, X., and M. Kuehlewind, "Innovating Transport with QUIC: Design Approaches and Research Challenges", IEEE Internet Computing, Vol 21(2), pp. 72-76 , March 2017, <https://mami-project.eu/wp-content/uploads/2017/03/QUIC.pdf>.

[draft-huitema-quic-dnsoquic-05]
Huitema, C., Shore, M., Mankin, A., Dickinson, S., and J. Iyengar, "Specification of DNS over Dedicated QUIC Connections (work in progress)", June 2018, <https://tools.ietf.org/html/draft-huitema-quic-dnsoquic-05>.

[draft-huitema-quic-mpath-req-01]
Huitema, C., "QUIC Multipath Requirements (work in progress)", January 2018, <https://tools.ietf.org/html/draft-huitema-quic-mpath-req-01>.

[draft-ietf-quic-invariants-01]
Thomson, M., "Version-Independent Properties of QUIC (work in progress)", March 2018, <https://tools.ietf.org/html/draft-ietf-quic-invariants-01>.

[draft-ietf-quic-spin-exp-00]
Trammell, B. and M. Kuehlewind, "The QUIC Latency Spin Bit (work in progress)", April 2018, <https://tools.ietf.org/html/draft-ietf-quic-spin-exp-00>.

[draft-ietf-quic-tls-12]
Thomson, M. and S. Turner, "Using Transport Layer Security (TLS) to Secure QUIC (work in progress)", May 2018, <https://tools.ietf.org/html/draft-ietf-quic-tls-12>.

[draft-ietf-quic-transport-12]
Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport (work in progress)", May 2018, <https://tools.ietf.org/html/draft-ietf-quic-transport-12>.

[draft-joseph-quic-comparison-quic-sctp-00]
Joseph, A., Li, T., He, Z., Cui, Y., and L. Zhang, "A Comparison Between SCTP and QUIC (work in progress)", March 2018, <https://tools.ietf.org/html/draft-joseph-quic-comparison-quic-sctp-00>.

[FIArch] Future Internet Architecture (FIArch) Group, "Future Internet Design Principles", January 2012, <https://pdfs.semanticscholar.org/0f33/5e6df68193367b0d0ea5430c043919477508.pdf>.

[Gratzer] Gratzer, F., ""QUIC - Quick UDP Internet Connections"", Seminar Innovative Internet-Technologien und Mobilkommunikation SS2016 , 2016, <https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2016-09-1/NET-2016-09-1_06.pdf>.

[Halletal] Hall, J., Aaron, M., and B. Jones, "A Survey of Worldwide Censorship Techniques (work in progress)", April 2015, <https://tools.ietf.org/html/draft-hall-censorship-tech-01>.

[Huston] Huston, G., "Just One QUIC Bit", APNIC , March 2018, <https://blog.apnic.net/2018/03/28/just-one-quic-bit/>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", December 1966, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>.

[ICESCR] United Nations General Assembly, "International Covenant on Economic, Social and Cultural Rights", December 1966, <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>.

[Kuehlewindetal] Kuehlewind, M., Buehler, T., Trammell, B., Neuhaus, S., Muentener, R., and G. Fairhurst, "A Path Layer for the Internet: Enabling Network Operations on Encrypted Protocols", IEEE International Conference on Network and Service Management (CNSM) , November 2017, <https://nsg.ee.ethz.ch/fileadmin/user_upload/CNSM_2017.pdf>.

[MolaviKakhkietal] Molavi Kakhki, A., Jero, S., Choffnes, D., Nita-Rotaru, C., and A. Mislove, "Taking a Long Look at QUIC", Proceedings of IMC '17, London, United Kingdom , November 2017, <https://david.choffnes.com/pubs/long-look-at-quic-imc17.pdf>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <https://www.rfc-editor.org/info/rfc1958>.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <https://www.rfc-editor.org/info/rfc2775>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC3724] Kempf, J., Ed., Austein, R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <https://www.rfc-editor.org/info/rfc3724>.

[RFC4084] Klensin, J., "Terminology for Describing Internet Connectivity", BCP 104, RFC 4084, DOI 10.17487/RFC4084, May 2005, <https://www.rfc-editor.org/info/rfc4084>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <https://www.rfc-editor.org/info/rfc4960>.

[RFC6582] Henderson, T., Floyd, S., Gurtov, A., and Y. Nishida, "The NewReno Modification to TCP's Fast Recovery Algorithm", RFC 6582, DOI 10.17487/RFC6582, April 2012, <https://www.rfc-editor.org/info/rfc6582>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E. Nordmark, "Technical Considerations for Internet Service Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754, March 2016, <https://www.rfc-editor.org/info/rfc7754>.

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>.

[RFC8404] Moriarty, K., Ed. and A. Morton, Ed., "Effects of Pervasive Encryption on Operators", RFC 8404, DOI 10.17487/RFC8404, July 2018, <https://www.rfc-editor.org/info/rfc8404>.

[Trammell01] Trammell, B., "Explicit Passive Measurability and the QUIC Spin Bit", APNIC , May 2018, <https://blog.apnic.net/2018/05/11/explicit-passive-measurability-and-the-quic-spin-bit/>.

[Trammell02] Trammell, B., "And Yet, It Spins", March 2018, <https://trammell.ch/post/2018-03-29-and-yet-it-spins>.

[UDHR] United Nations General Assembly, "The Universal Declaration of Human Rights", December 1948, <http://www.un.org/en/documents/udhr/>.

[Wilketal] Wilk, A., Hamilton, R., and I. Swett, "A QUIC Update on Google's Experimental Transport", April 2015, <https://blog.chromium.org/2015/04/a-quic-update-on-googles-experimental.html>.

[Ziewitzetal] Ziewitz, M. and I. Brown, "A Prehistory of Internet Governance", Research Handbook on Governance of the Internet, ed I. Brown, 3-26. Cheltenham: Edward Elgar , 2013.

10.2. URIs

[1] mailto:hr-rt@irtf.org

[2] https://www.irtf.org/mailman/listinfo/hr-rt

[3] https://www.irtf.org/mail-archive/web/hr-rt/current/index.html

Authors' Addresses

Beatrice Martini
Harvard Kennedy School

EMail: mail@beatricemartini.it

Niels ten Oever
University of Amsterdam

EMail: mail@nielstenoever.net

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 14, 2019

T. Pauly
E. Kinnear
D. Schinazi
Apple Inc.

September 10, 2018

An Unreliable Datagram Extension to QUIC
draft-pauly-quic-datagram-00

Abstract

This document defines an extension to the QUIC transport protocol to add support for sending and receiving unreliable datagrams over a QUIC connection.

Table of Contents

1. Introduction 2
1.1. Specification of Requirements 2
2. Motivation 2
3. Transport Parameter 3
4. Datagram Frame Type 3
5. Behavior and Usage 4
5.1. Flow Control and Acknowledgements 4
6. Security Considerations 5
7. IANA Considerations 5
8. Acknowledgments 5
9. Informative References 5
Authors' Addresses 6

1. Introduction

The QUIC Transport Protocol [I-D.ietf-quic-transport] provides a secure, multiplexed connection for transmitting reliable streams of application data. Reliability within QUIC is performed on a per-stream basis, so some frame types are not eligible for retransmission.

Some applications, particularly those that need to transmit real-time data, prefer to transmit data unreliably. These applications can build directly upon UDP [RFC0768] as a transport, and can add security with DTLS [RFC6347]. Extending QUIC to support transmitting unreliable application data would provide another option for secure datagrams, with the added benefit of sharing a cryptographic and authentication context used for reliable streams.

This document defines two new DATAGRAM QUIC frame types, which carry application data without requiring retransmissions.

1.1. Specification of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Motivation

Transmitting unreliable data over QUIC provides benefits over existing solutions:

- Applications that open both a reliable TLS stream and an unreliable DTLS flow to the same peer can benefit by sharing a single handshake and authentication context between a reliable QUIC stream and flow of unreliable QUIC datagrams. This can reduce the latency required for handshakes.

- QUIC uses a more nuanced loss recovery mechanism than the DTLS handshake, which has a basic packet loss retransmission timer. This may allow loss recovery to occur more quickly for QUIC data.

- QUIC datagrams, while unreliable, can support acknowledgements, allowing applications to be aware of if a datagram was successfully received.

These reductions in connection latency, and application insight into the delivery of datagrams, can be useful for optimizing audio/video streaming applications, gaming applications, and other real-time network applications.

Unreliable QUIC datagrams can also be used to implement an IP packet tunnel over QUIC, such as for a Virtual Private Network (VPN). Internet-layer tunneling protocols generally require a reliable and authenticated handshake, followed by unreliable secure transmission of IP packets. This can, for example, require a TLS connection for the control data, and DTLS for tunneling IP packets. A single QUIC connection could support both parts with the use of unreliable datagrams.

3. Transport Parameter

Support for receiving the DATAGRAM frame types is advertised by means of a QUIC Transport Parameter (name=accepts_datagrams, value=12). An endpoint that includes this parameter supports the DATAGRAM frame types and is willing to receive such frames on this connection. Endpoints MUST NOT send DATAGRAM frames until they have sent and received the accepts_datagrams transport parameter. An endpoint that receives a DATAGRAM frame when it has not sent the accepts_datagrams transport parameter MUST terminate the connection with error PROTOCOL_VIOLATION.

4. Datagram Frame Type

DATAGRAM frames are used to transmit application data in an unreliable manner. The DATAGRAM frame type takes the form 0b0001110X (or the set of values from 0x1c to 0x1d). The least significant byte of the DATAGRAM frame type is the LEN bit (0x01). It indicates that there is a Length field present. If this bit is set to 0, the Length

field is absent and the Stream Data field extends to the end of the packet. If this bit is set to 1, the Length field is present.

A DATAGRAM frame is shown below.

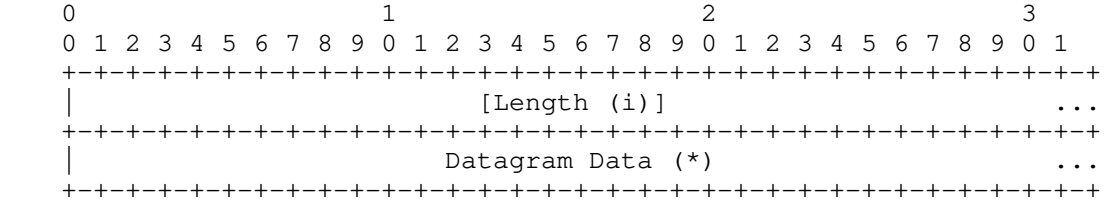

Figure 1: DATAGRAM Frame Format

The fields of a DATAGRAM frame are as follows:

Length: A variable-length integer specifying the length of the datagram in bytes. If the length is zero, the data extends to the end of the QUIC packet.

Datagram Data: The bytes of the datagram to be delivered.

5. Behavior and Usage

When an application sends an unreliable datagram over a QUIC connection, QUIC will generate a new DATAGRAM frame and send it in the first available packet. This frame SHOULD NOT be delayed, but MAY be coalesced with other STREAM or DATAGRAM frames.

When a QUIC endpoint receives a valid DATAGRAM frame, it SHOULD deliver the data to the application immediately.

DATAGRAM frames MUST be protected with either 0-RTT or 1-RTT keys.

Note that the DATAGRAM frame does not support identifying separate flows of datagrams within a single QUIC connection, as the Stream ID does for STREAM frames. Demultiplexing datagram data is the responsibility of the application.

5.1. Flow Control and Acknowledgements

Although the DATAGRAM frame is not retransmitted upon loss detection, it does contribute to the maximum data for the overall connection. Packets that contain only DATAGRAM frames do need to be acknowledged, but implementations SHOULD defer and batch acknowledgements since the timing of these acknowledgements is not used for loss recovery.

The DATAGRAM frame does not provide any explicit flow control signaling apart from the connection-level flow control. DATAGRAM frames are flow controlled only when the maximum data for the connection is hit, at which point the BLOCKED frame is sent.

In cases in which a DATAGRAM frame is blocked due to connection-level flow control or congestion control, an implementation MAY drop the frame without sending it.

6. Security Considerations

The DATAGRAM frame shares the same security properties as the rest of the data transmitted within a QUIC connection. All application data transmitted with the DATAGRAM frame, like the STREAM frame, MUST be protected either by 0-RTT or 1-RTT keys.

7. IANA Considerations

This document registers a new value in the QUIC Transport Parameters:

Value: 12 (if this document is approved)

Parameter Name: accepts_datagrams

Specification: Indicates that the connection should enable support for unreliable DATAGRAM frames. An endpoint that advertises this transport parameter can receive datagrams frames from the other endpoint.

This document also registers a new value in the QUIC Frame Type registry:

Value: 0x1c - 0x1d (if this document is approved)

Frame Name: DATAGRAM

Specification: Unreliable application data

8. Acknowledgments

Thanks to Ian Swett, who inspired this proposal.

9. Informative References

[I-D.ietf-quic-transport]
Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport", draft-ietf-quic-transport-14 (work in progress), August 2018.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <https://www.rfc-editor.org/info/rfc768>.

[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>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: tpauly@apple.com

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: ekinnear@apple.com

David Schinazi
Apple Inc.
One Apple Park Way
Cupertino, California 95014
United States of America

Email: dschinazi@apple.com