Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica (Classe L-31)

Il protocollo QUIC, a multiplexed transport over UDP – The Chromium Project

Laureando
Andrea Pastuglia

Matricola 110679

Relatore
Fausto Marcantoni

A.A. 2022/2023

Indice

Elenco delle figure

1. Introduzione

1.1 Sommario

Nell'epoca sempre più interconnessa delle comunicazioni digitali, il costante progresso delle tecnologie ha reso fondamentale l'adattamento dei protocolli di trasporto per soddisfare le crescenti esigenze delle applicazioni web. In quest'ottica, il protocollo QUIC (Quick UDP Internet Connections), introdotto attraverso il progetto Chromium, emerge come una soluzione avanzata e promettente.

1.1.1 Contestualizzazione del Panorama dei Protocolli di Trasporto

La comunicazione su Internet è stata storicamente regolamentata da protocolli di trasporto come TCP e UDP. TCP offre una connessione affidabile e orientata alla connessione, ideale per applicazioni che richiedono una consegna senza perdite e in ordine dei dati, come le transazioni finanziarie online. D'altra parte, UDP è orientato alla connessione e fornisce un servizio più leggero, adatto per applicazioni in cui la tempestività è prioritaria rispetto alla consegna affidabile. [Com13]

Tuttavia, con l'evoluzione del panorama digitale, le esigenze sono cambiate. Applicazioni moderne, come streaming video, giochi online e servizi basati su cloud, richiedono una combinazione di prestazioni elevate, bassa latenza e flessibilità nella gestione dei dati. In questo contesto, il protocollo QUIC emerge come un'alternativa rivoluzionaria che punta a conciliare la sicurezza e le prestazioni, introducendo un nuovo paradigma di trasporto su UDP.

L'analisi critica dei protocolli tradizionali, insieme alla crescente domanda di efficienza e sicurezza, ha spinto gli sviluppatori a cercare soluzioni innovative. QUIC è stato concepito come risposta a questa esigenza, integrando molte funzionalità avanzate, tra cui il multiplexing e una gestione intelligente della connessione, per migliorare l'esperienza dell'utente finale.

L'importanza di questa ricerca risiede nell'esplorazione di come QUIC, in combinazione con il progetto Chromium, possa riscrivere le dinamiche della comunicazione su Internet, superando le limitazioni intrinseche dei protocolli tradizionali e offrendo una soluzione più adatta alle esigenze della nuova connettività digitale.

1.1.2 Importanza della Ricerca su QUIC nel Contesto Attuale

L'adozione sempre più diffusa di applicazioni web complesse e il continuo sviluppo di tecnologie emergenti pongono l'accento sulla necessità di protocolli di trasporto più avanzati. La ricerca su QUIC non solo contribuisce a un migliore comprensione della sua architettura e funzionalità, ma anche a una visione più ampia di come tali innovazioni impattino sulle dinamiche dell'ecosistema web.

Questo approfondimento è essenziale per fornire una base solida per la valutazione dell'efficacia di QUIC nel contesto del progetto Chromium e per delineare scenari futuri in cui il protocollo può svolgere un ruolo centrale. La ricerca non si limita a un mero esame tecnico, ma si estende anche a considerazioni pratiche e applicative, garantendo una prospettiva completa sull'importanza di QUIC nel contesto attuale.

1.2 Scopo ed obiettivo della tesi

L'obiettivo di questo tesi è quello di esplorare approfonditamente il protocollo QUIC, con particolare ricerca sul suo ruolo all'interno del progetto Chromium. L'indagine mira a fornire una panoramica completa delle caratteristiche distintive del protocollo, dall'analisi approfondita delle sue fondamenta di progettazione al contesto storico del suo sviluppo.

La storia di QUIC, originatasi all'interno di Google e successivamente standardizzata dall'IETF, rappresenta una fase cruciale nel percorso evolutivo del protocollo. Il coinvolgimento di Chromium è un elemento chiave, poiché il progetto agisce come catalizzatore nello sviluppo pratico e nell'adozione di QUIC. La tesi esplorerà in dettaglio come Chromium contribuisce attivamente a plasmare il protocollo e facilita la sua integrazione nei browser di ampia diffusione. [JI21b]

Una parte significativa dell'analisi sarà dedicata alle differenze sostanziali tra QUIC e i protocolli tradizionali come TCP e UDP. Questo approfondimento comprenderà la gestione del multiplexing, il processo di handshake, l'integrazione della sicurezza, la capacità di recovery degli errori e la progettazione adattabile di QUIC, mettendo in evidenza le innovazioni che rendono QUIC una soluzione avanzata rispetto ai protocolli convenzionali.

Un'attenzione particolare sarà dedicata ai vantaggi che QUIC porta nell'ambito delle comunicazioni web, risolvendo problematiche chiave e offrendo miglioramenti significativi in termini di efficienza e sicurezza. Tuttavia, verranno anche esplorate criticamente le possibili sfide e problematiche legate all'implementazione e all'adozione di QUIC.

La tesi si spingerà oltre l'analisi tecnica, esaminando le applicazioni pratiche di QUIC in Chromium e proponendo possibili sviluppi futuri del protocollo. Inoltre, sarà dedicato uno sguardo approfondito alla sicurezza, esplorando i principi e i meccanismi implementati sia in QUIC che all'interno del Chromium Project.

2. Fondamenti Teorici

2.1 Concetti di base sui protocolli di trasporto

I protocolli di trasporto costituiscono il fondamento della comunicazione dati nelle reti informatiche, fornendo il supporto necessario per il trasferimento affidabile e ordinato delle informazioni tra due o più dispositivi connessi. Tra i protagonisti di questo ambito, spiccano il Transmission Control Protocol (TCP) e l'User Datagram Protocol (UDP).

Il TCP è un protocollo orientato alla connessione, progettato per garantire la sicurezza e l'integrità dei dati trasmessi. Utilizza un sistema di acknowledgment, in cui il destinatario conferma la ricezione dei dati inviati, e impiega meccanismi di ritrasmissione in caso di perdita di informazioni. Inoltre, TCP si occupa di gestire l'ordine di arrivo dei dati per garantire la corretta ricostruzione dell'informazione originale. [Com13]

D'altra parte, l'UDP si distingue come un protocollo senza connessione, caratterizzato dalla sua immediatezza e leggerezza. Non offre garanzie di affidabilità e ordine, ma compensa tale mancanza con una minore latenza e un overhead ridotto. È particolarmente adatto per applicazioni in cui la tempestività della trasmissione è prioritaria rispetto alla corretta sequenza o alla consegna affidabile dei dati. [Com13]

Questi protocolli rappresentano approcci differenti alla comunicazione di rete, con TCP focalizzato sull'affidabilità e l'UDP orientato alla rapidità. La scelta tra essi dipende dalle esigenze specifiche dell'applicazione e dalle condizioni della rete in cui vengono impiegati.

2.2 Storia dello sviluppo di QUIC

La storia dello sviluppo di QUIC rappresenta una tappa significativa nella continua evoluzione dei protocolli di trasporto. Nel contesto di un mondo digitale sempre più interconnesso, la necessità di migliorare le prestazioni e l'efficienza delle comunicazioni online ha guidato lo sviluppo di nuovi approcci. QUIC, acronimo di "Quick UDP Internet Connections," è emerso come una risposta innovativa a queste esigenze.

Il percorso di sviluppo di QUIC ha origine all'interno di Google, con gli ingegneri Jana Iyengar e Ian Swett, che iniziarono a esplorare nuove vie per ottimizzare la trasmissione di dati su Internet. Nel 2012, Google ha presentato QUIC come proposta sperimentale, abbracciando UDP come protocollo di trasporto anziché utilizzare TCP.

Uno degli obiettivi principali di QUIC era superare alcune limitazioni di TCP, come la necessità di diversi round trip per stabilire una connessione. QUIC ha affrontato questo problema introducendo il concetto di handshake zero-RTT (Zero Round-Trip Time).

Questo handshake è stato ideato apposta per ottimizzare la creazione di connessio-

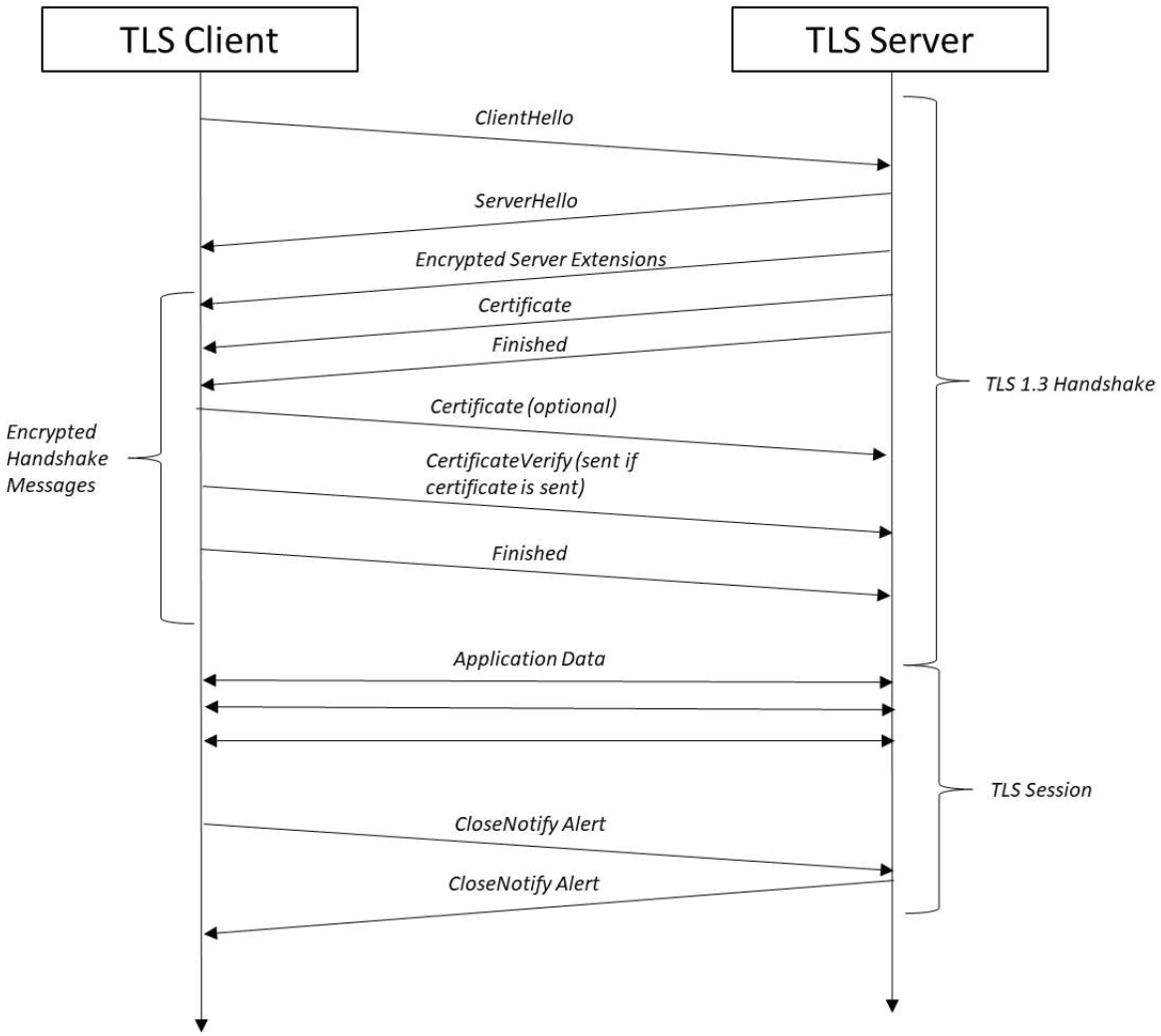

Figura 2.1: Handshake zero-RTT[Fot]

ni, riducendo il tempo di latenza necessario per stabilire una connessione sicura tra un client e un server. In un normale handshake, ci sono di solito una o più fasi di scambio di messaggi tra il client e il server prima che la connessione sia completamente stabilita. Questi messaggi richiedono round-trip tra il client e il server, aumentando il tempo totale necessario per iniziare la trasmissione di dati. Come si vede in figura 2.1 l'handshake zero-RTT, QUIC consente al client di iniziare a inviare dati nella prima transazione di round-trip, senza dover attendere il completamento dell'intero processo di handshake. Questo significa che il client può inviare dati già nella prima interazione, riducendo significativamente il tempo totale necessario per avviare la comunicazione. [JI21a]

QUIC ha attraversato un significativo percorso evolutivo, con la sua origine all'interno di Google e una fase di sviluppo iniziale mirata a migliorare le prestazioni delle comunicazioni su Internet. Nel 2015, l'IETF ha avviato il processo di standardizzazione di QUIC, aprendo la porta a un coinvolgimento più ampio della comunità tecnica al di là di Google.[JI21b]

Negli anni successivi, sono state apportate numerose revisioni e miglioramenti al protocollo, riflettendo un approccio dinamico e iterativo. L'obiettivo era perfezionare

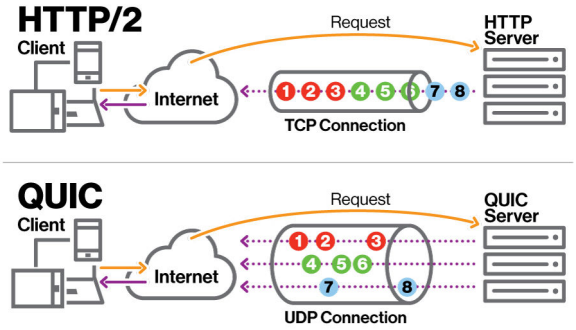

Figura 2.2: [Htt]

le caratteristiche del protocollo, migliorarne la sicurezza e ottimizzare l'efficienza in una varietà di scenari di utilizzo.

Il culmine di questo percorso evolutivo è stato raggiunto con la standardizzazione di QUIC versione 1 da parte dell'IETF nel 2020. Questo passo ha conferito a QUIC uno status ufficiale come protocollo di trasporto standard, stabilendo una base comune e unificata per la sua implementazione globale. Parallelamente, QUIC è stato progettato per funzionare in tandem con HTTP/3, il protocollo di applicazione, creando un'esperienza avanzata e ottimizzata per le comunicazioni web. [Bis22]

La standardizzazione non solo consolida la presenza di QUIC nel panorama delle comunicazioni su Internet, ma contribuisce anche a coerenza, interoperabilità e sicurezza. L'evoluzione di QUIC rappresenta una risposta alle esigenze mutevoli del mondo digitale e offre un nuovo standard per le prestazioni e l'efficienza nella trasmissione dei dati online.

2.3 Descrizione di modifiche e sviluppi dello standard di QUIC

Lo standard di QUIC, inizialmente sviluppato da Google nel 2012 e successivamente adottato dall'IETF (Internet Engineering Task Force) come base per un nuovo standard di Internet, ha subito un'evoluzione significativa nel corso degli anni. Questo processo di standardizzazione e sviluppo ha mirato a rendere QUIC un protocollo di trasporto più efficiente, sicuro e affidabile per l'uso su Internet. Le modifiche e gli sviluppi dello standard di QUIC riflettono un impegno continuo verso l'ottimizzazione delle prestazioni di rete e l'adattabilità alle esigenze delle moderne applicazioni web.

2.3.1 Origini e Sviluppi Iniziali

QUIC è stato originariamente progettato per superare le limitazioni di TCP e UDP, combinando la bassa latenza di UDP con meccanismi di controllo del flusso e affidabilità simili a quelli di TCP. La versione iniziale di QUIC implementata da Google si concentrava principalmente sul miglioramento delle prestazioni delle applicazioni web, riducendo la latenza di connessione attraverso un processo di handshake più efficiente e introducendo il concetto di multiplexing senza blocco di testa di linea per le connessioni HTTP/2.

2.3.2 La Transizione verso l'IETF e la Standardizzazione

La transizione di QUIC da un progetto Google a uno standard proposto dall'IETF ha segnato una tappa cruciale nello sviluppo del protocollo. L'IETF ha avviato il lavoro sul QUIC come standard aperto, portando a significative revisioni e miglioramenti. Questo processo ha incluso un'ampia collaborazione tra aziende, organizzazioni e individui, con l'obiettivo di creare un protocollo di trasporto versatile e robusto per il futuro di Internet.

2.3.3 Innovazioni Chiave nello Standard IETF di QUIC

Crittografia Integrata

A differenza di TCP, che si appoggia a TLS per la sicurezza, QUIC integra la crittografia direttamente nel protocollo, utilizzando TLS 1.3. Questo non solo semplifica la pila di protocolli ma garantisce anche che tutte le comunicazioni QUIC siano protette da ascolti indesiderati fin dall'inizio.

Miglioramenti nella Gestione della Congestione

QUIC introduce algoritmi di controllo della congestione più avanzati, progettati per essere più reattivi alle condizioni di rete in rapida evoluzione, migliorando così la velocità e l'affidabilità delle trasmissioni.

Indipendenza dal Flusso

La capacità di QUIC di gestire i flussi di dati in modo indipendente all'interno della stessa connessione riduce significativamente il problema del blocco di testa di linea, consentendo una trasmissione dei dati più efficiente e affidabile.

Miglioramento del Handshake

QUIC riduce il numero di round-trip necessari per stabilire una connessione, grazie all'utilizzo di chiavi pre-condivise in sessioni successive. Questo accelera significativamente l'apertura delle connessioni, particolarmente utile in ambienti mobili dove i round-trip possono essere costosi in termini di tempo.

Supporto per la Mobilità

QUIC è progettato per gestire meglio i cambiamenti dell'indirizzo IP, permettendo alle connessioni di persistere anche quando un utente cambia rete. Questa caratteristica è essenziale nell'era degli smartphone e della connettività mobile.

2.4 Che cos'è "The Chromium Project"

"The Chromium Project" rappresenta un ambizioso sforzo di sviluppo open source condotto da Google, focalizzato principalmente sulla creazione e l'evoluzione del browser web Google Chrome. Questo progetto è stato avviato con l'obiettivo di creare un browser web open-source, veloce, sicuro e stabile. Il nome "Chromium" deriva dal metallo

Figura 2.3: Stemma chromium[Ste]

cromato, che è un componente del legame del cromo utilizzato per proteggere l'acciaio dalla corrosione, simboleggiando così l'intento di fornire un browser web robusto e resistente.

La base di Chromium è costituita dal motore di rendering Blink, che è stato biforcato da WebKit nel 2013. Questo motore di rendering gestisce la visualizzazione delle pagine web, garantendo un'esperienza utente fluida e conforme agli standard web moderni.

Una delle caratteristiche distintive di Chromium è la sua natura open-source, che permette a sviluppatori indipendenti di contribuire attivamente al suo sviluppo e miglioramento. Ciò ha portato alla creazione di una vasta comunità di sviluppatori, che lavorano insieme per identificare bug, introdurre nuove funzionalità e ottimizzare le prestazioni del browser.

Chromium serve anche da base per diversi altri browser web, tra cui il popolare Google Chrome. Google Chrome è essenzialmente un'implementazione di Chromium arricchita con funzionalità aggiuntive come la sincronizzazione dei dati con il proprio account Google e l'integrazione di servizi Google come la ricerca e il traduttore.

Inoltre, Chromium non è limitato solo ai browser web. Il progetto ha anche portato alla creazione di altri prodotti e progetti, tra cui Chrome OS, un sistema operativo leggero basato su Linux progettato per l'utilizzo su dispositivi come Chromebooks. [Goo08]

2.5 Differenze tra Chrome e Chromium

Sia google Chrome che chromium Chromium emergono dallo stesso ceppo di sviluppo, condividendo gran parte del loro DNA digitale, ma divergono molto quando si tratta delle loro filosofie di implementazione, delle funzionalità offerte e delle loro implicazioni per la privacy degli utenti. Mentre Chromium fornisce una base di codice che chiunque nel mondo può esplorare, modificare e distribuire, Google Chrome spicca come la faccia principale di questo impegno, con tante funzioni speciali e ben collegato agli altri servizi di Google.

La nascita di Chromium avviene per contribuire a un web aperto e accessibile, un

	Google Chrome	Chromium
Logo	Colorato	Blu
Segnalazione crash	Sì, se è abilitato	No
User metrics (invio statistiche sull'uso del programma)	Sì, se è abilitato	No
tag <audio> e <video> di HTML5	H.264, AAC, MP3, Vorbis e Theora	Vorbis e Theora
Traduzione pagine web	Sì	Sì
Codice	Testato dagli sviluppatori	Modificato dalle distribuzioni
Sandbox	Sempre attivata	Dipende dalla distribuzione (Ubuntu e Gentoo sì)
Pacchetti	singolo pacchetto deb o rpm	Dipende dalla distribuzione. Spesso il programma è diviso in diversi pacchetti
Profilo	Salvato in `~/.config/google-chrome`	Salvato in `~/.config/chromium`

Figura 2.4: tabella differenze tra chrome e chromium[Difa]

Profilo	Salvato in `~/.config/google-chrome`	Salvato in `~/.config/chromium`
Cache	Salvato in `~/.cache/google-chrome`	Salvato in `~/.cache/chromium`
Controllo di qualità	Solo versioni stabili: i nuovi rilasci sono testati prima di essere distribuiti	Dipende dalla distro e dal repository usato
Flash Player Integrato	Sì	No
Licenze	EULA	licenza BSD con altre parti soggette a varie licenze libere

Figura 2.5: tabella differenze tra chrome e chromium[Difb]

progetto che serve da base per un'ampia gamma di browser, permettendo loro di adattarsi a specifiche esigenze di privacy, sicurezza e funzionalità. Al contrario, Google Chrome rappresenta l'ambizione di Google di offrire un'esperienza utente senza soluzione di continuità, arricchita da aggiornamenti automatici, supporto per formati video e audio proprietari, e una stretta integrazione con i suoi servizi, dall'autenticazione Google alla sincronizzazione tra dispositivi. Queste aggiunte, sebbene migliorino l'usabilità e l'efficienza per l'utente finale, sollevano questioni riguardanti la raccolta di dati e la personalizzazione degli annunci pubblicitari, evidenziando un compromesso tra comodità e privacy.

La differenza principale tra Chromium e Chrome si manifesta nelle loro approcci alla privacy e alla sicurezza. L'open-source di Chromium invita a una trasparenza che viene apprezzata da molti utenti, permettendo un esame approfondito del codice per assicurarsi che non ci siano sorprese nascoste o meccanismi di tracciamento ingiustificati. dall'altra parte, Chrome, pur essendo all'avanguardia nella protezione contro minacce online e nell'offrire aggiornamenti frequenti per combattere vulnerabilità emergenti, ingloba in se anche elementi che facilitano la raccolta di dati per Google, aumentando il suo ecosistema pubblicitario. Questo aspetto di Chrome, mentre supporta l'offerta di servizi gratuiti e personalizzati, pone domande sulla quantità e il tipo di dati raccolti e su come vengono utilizzati.

Scegliere tra Chrome e Chromium è quindi una decisione che dipende dalle priorità personali di un utente in termini di funzionalità, convenienza, e considerazioni sulla privacy. Chrome offre un'esperienza utente ricca e integrata, con pochi compromessi sulla comodità e l'accesso a un'ampia gamma di servizi web. D'altra parte, Chromium attira coloro che valorizzano la trasparenza, il controllo personalizzato e una maggiore attenzione alla privacy, anche se ciò richiede un maggiore impegno nell'aggiornamento e nella configurazione del browser. In definitiva, sia Chrome che Chromium hanno contribuito in modo significativo all'evoluzione di Internet, offrendo agli utenti la libertà

di scegliere un percorso che dipene dalle loro esigenze.

2.6 Il Contributo Significativo di Chromium nello Sviluppo e nell'Avanzamento di QUIC

Chromium svolge un ruolo fondamentale nell'ecosistema di sviluppo di QUIC, offrendo un terreno fertile per l'adozione, la sperimentazione e l'ottimizzazione continua di questo avanzato protocollo di trasporto. L'interazione sinergica tra Chromium e QUIC si articola in diverse dimensioni, evidenziando la stretta connessione tra un browser ampiamente utilizzato e l'evoluzione dei protocolli di comunicazione su Internet.

Innanzitutto, Chromium agisce come una piattaforma di test dinamica, permettendo agli sviluppatori di Google e alla comunità open source di integrare le versioni più recenti di QUIC. Questo ambiente di test offre l'opportunità di identificare e risolvere eventuali problematiche, garantendo che il protocollo sia robusto e conforme agli standard di sicurezza prima di essere implementato su larga scala. L'iterazione continua in questo ambiente di sviluppo contribuisce a rifinire costantemente QUIC, mantenendolo all'avanguardia delle esigenze di una comunicazione online sempre più complessa.

Oltre a fungere da campo di prova, Chromium fornisce una vetrina per le capacità di QUIC. L'implementazione del protocollo in un browser di ampia diffusione, come Chrome, non solo dimostra la praticità di QUIC ma offre anche dati empirici sulla sua efficienza in condizioni reali di utilizzo. Questa valutazione pratica è essenziale per un ciclo di sviluppo iterativo, permettendo agli sviluppatori di apportare miglioramenti mirati basati su esperienze reali di navigazione web.

La sinergia tra Chromium e QUIC si estende ulteriormente alla sua influenza sul panorama dei browser web. La posizione predominante di Chromium come base di diversi browser, oltre a Chrome stesso, amplifica l'impatto di QUIC. La visibilità e la credibilità di Chromium contribuiscono a spingere altri browser a implementare e adottare QUIC, accelerando la sua diffusione come standard rilevante per le comunicazioni online su scala globale.

Da un punto di vista più ampio, il coinvolgimento di Chromium nello sviluppo di QUIC sottolinea il ruolo cruciale del browser come interfaccia chiave tra gli utenti e le tecnologie web. L'integrazione di nuovi protocolli all'avanguardia, come QUIC, all'interno di un browser di ampia diffusione non solo influisce direttamente sull'esperienza degli utenti ma contribuisce anche a plasmare l'evoluzione futura delle comunicazioni web.

In conclusione, Chromium non è semplicemente un implementatore tecnico di QUIC, ma un catalizzatore che accelera la sua adozione, contribuendo attivamente a definire il futuro delle comunicazioni su Internet attraverso l'incorporazione e il sostegno di tecnologie all'avanguardia.

2.7 Differenze tra QUIC e Protocolli Tradizionali (TCP, UDP)

L'esame delle differenze tra QUIC e i protocolli tradizionali, come TCP e UDP, rivela le innovazioni e le ottimizzazioni che hanno guidato lo sviluppo di QUIC per affrontare specifiche sfide nel contesto delle comunicazioni su Internet.

2.7.1 Approccio al Multiplexing e Flusso dei Dati

QUIC si distingue per l'approccio avanzato al multiplexing, consentendo la trasmissione simultanea di più flussi di dati su una singola connessione. Questo si contrappone a TCP, che richiede la creazione di diverse connessioni per gestire flussi distinti. L'efficienza del multiplexing di QUIC risulta in una riduzione dei tempi di caricamento delle pagine web, contribuendo a una navigazione più fluida.

2.7.2 Handshake e Connessione Iniziale

QUIC introduce un "handshake zero-RTT" che consente una connessione più rapida rispetto a TCP, che richiede diversi round trip per stabilire una connessione. Questo aspetto rende QUIC particolarmente adatto per applicazioni che richiedono una connessione immediata, migliorando l'esperienza dell'utente all'avvio di sessioni di comunicazione.

2.7.3 Integrazione di Sicurezza

Una delle differenze chiave è la gestione della sicurezza. Mentre TCP richiede l'implementazione di TLS separatamente per garantire la sicurezza delle comunicazioni, QUIC incorpora nativamente il protocollo di sicurezza TLS. Questa integrazione contribuisce a una maggiore sicurezza delle trasmissioni, semplificando al contempo l'implementazione per gli sviluppatori.

2.7.4 Gestione degli Errori e Recovery

QUIC presenta meccanismi avanzati di gestione degli errori e recovery, affrontando le perdite di dati in modo più efficiente rispetto a TCP. L'implementazione di meccanismi come il "loss recovery" contribuisce a mantenere una connessione stabile anche in presenza di condizioni di rete variabili.

2.7.5 Adattabilità e Miglioramenti Continui

A differenza dei protocolli tradizionali, QUIC è stato progettato per permettere aggiornamenti e miglioramenti senza la necessità di modifiche significative all'infrastruttura. Questa caratteristica di adattabilità facilita l'evoluzione del protocollo in risposta alle nuove esigenze e alle sfide emergenti.

In conclusione, le differenze tra QUIC e i protocolli tradizionali come TCP e UDP riflettono un approccio innovativo per migliorare le prestazioni, la sicurezza e l'efficienza delle comunicazioni su Internet. L'adozione di QUIC segna una pietra miliare nell'evoluzione dei protocolli di trasporto, influenzando positivamente l'esperienza degli utenti e la dinamica delle comunicazioni web.

Caratteristica	QUIC	TCP	UDP
Handshake	Handshake zero-RTT per ridurre la latenza	Handshake a tre vie (3-way handshake)	Nessun handshake
Multiplexing	Multiplexing integrato	No	No
Connessione Persistente	Sì	Sì	No
Controllo della Congestione	Implementato	Implementato	Implementato
Gestione della Perdita Pacchetti	Implementato	Implementato	Non implementato
Rinnovo delle Chiavi	Sì	No	No
Estensibilità	Sì	No	No
Supporto Applicazioni	Sì	Sì	Sì

Tabella 2.1: Differenze tra QUIC, TCP e UDP

3. Architettura di QUIC

3.1 Struttura generale e Componenti del protocollo QUIC

QUIC (Quick UDP Internet Connections) rappresenta un'innovazione significativa nel campo dei protocolli di trasporto su Internet, cercando di superare le limitazioni dei protocolli tradizionali come TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) attraverso una struttura e dei componenti che offrono miglioramenti in termini di velocità, sicurezza, efficienza e affidabilità delle comunicazioni online. La struttura generale di QUIC e i suoi componenti principali vengono da un'attenta progettazione orientata a soddisfare le esigenze delle moderne applicazioni web e dei servizi Internet.

3.1.1 Struttura Generale di QUIC

QUIC è un protocollo di trasporto basato su UDP che incorpora numerosi miglioramenti per ottimizzare la consegna dei dati su Internet. A differenza di TCP, QUIC riduce la latenza attraverso un processo di handshake più efficiente e gestisce la perdita di pacchetti e la congestione in modo più sofisticato. La sua struttura è progettata per essere sicura, multiplexata e adattabile alle variazioni delle condizioni di rete, offrendo una base solida per il traffico Internet che richiede elevate prestazioni e affidabilità.

3.1.2 Componenti Principali del Protocollo QUIC

Handshake Efficiente e Connessioni

L'innovazione portata da QUIC nel processo di handshake e gestione delle connessioni rappresenta una delle sue caratteristiche distintive, che si traduce in un miglioramento tangibile delle prestazioni rispetto ai tradizionali protocolli di rete. Al centro di questa innovazione c'è l'obiettivo di ridurre al minimo la latenza nell'avvio delle connessioni, un aspetto critico per le moderne applicazioni web che vogliono interazioni rapide e fluide con gli utenti. La progettazione dell'handshake di QUIC cerca di superare le inefficienze legate all'avvio delle connessioni in TCP, dove il processo di handshake a tre vie e la successiva negoziazione TLS possono introdurre ritardi significativi prima che i dati inizino effettivamente a fluire.

QUIC implementa un meccanismo di handshake che sfrutta la crittografia integrata per stabilire connessioni sicure con un numero ridotto di scambi di messaggi. Per le nuove connessioni, QUIC può completare l'handshake e iniziare la trasmissione dei dati in un solo round-trip (1-RTT), un miglioramento significativo rispetto ai processi multi-step richiesti da TCP e TLS. Ancora più impressionante è la capacità di QUIC di effettuare connessioni successive tra gli stessi endpoint praticamente istantanee, uti-

lizzando il meccanismo 0-RTT che sfrutta le chiavi crittografiche pre-condivise dalle sessioni precedenti. Questo approccio non solo accelera l'apertura delle connessioni ma riduce anche la latenza percepita dall'utente, migliorando l'esperienza generale su siti web e applicazioni. [Ghe19]

Al di là della velocità, la gestione delle connessioni in QUIC è progettata per essere incredibilmente resiliente. Utilizzando identificatori di connessione unici invece che l'abbinamento tradizionale di indirizzi IP e porte, QUIC permette alle connessioni di persistere anche quando un dispositivo cambia rete o indirizzo IP. Questa capacità non solo evita interruzioni delle sessioni attive ma assicura anche una transizione fluida e senza soluzione di continuità tra reti diverse, migliorando l'affidabilità delle comunicazioni su dispositivi mobili.

Inoltre, l'architettura di QUIC incorpora meccanismi per prevenire attacchi di tipo replay sui pacchetti 0-RTT. Cosi facendo bilancia l'esigenza di velocità con quella della sicurezza delle connessioni. La combinazione di questi elementi (l'handshake ottimizzato, la resilienza delle connessioni e la sicurezza integrata) evidenzia come QUIC sia stato attentamente progettato per rispondere alle esigenze di un Internet sempre più dinamico e interconnesso, ponendo le basi per un'esperienza utente notevolmente migliorata rispetto ai protocolli di rete precedenti.[JI21a]

Crittografia Integrata

Al contrario di TCP, che ha bisogno di strati supplementari come TLS per garantire la sicurezza delle comunicazioni, QUIC incorpora la crittografia all'interno del suo design, assicurando che ogni singolo bit di dati trasmesso sia automaticamente protetto da occhi indiscreti fin dall'inizio della connessione. Questa integrazione della crittografia, che si basa sul robusto standard TLS 1.3, offre un'ottimo livello di sicurezza e privacy.

Con QUIC, la negoziazione delle chiavi crittografiche e la cifratura dei dati avvengono simultaneamente all'instaurazione della connessione, eliminando le vulnerabilità associate ai ritardi e alle complessità degli handshake separati per la sicurezza, tipici dell'accoppiamento TCP/TLS.

Inoltre, l'integrazione della crittografia in QUIC non si limita a proteggere il contenuto dei dati trasmessi, ma estende la sua copertura anche agli elementi di controllo della connessione, come la gestione del flusso e la correzione degli errori. Questo approccio alla sicurezza garantisce che informazioni potenzialmente sensibili, come la struttura del traffico e i pattern di comunicazione, siano protette tanto quanto i dati stessi, offrendo una barriera robusta contro una quantità elevata di possibilità di attacco.

La crittografia integrata in QUIC migliora in modo significativo anche l'efficienza della negoziazione crittografica. Visto che la sicurezza è incorporata direttamente nel processo di handshake del protocollo, QUIC riduce il numero di round-trip necessari per stabilire una connessione protetta, accelerando le comunicazioni e migliorando l'esperienza utente. Questo è molto vantaggioso in scenari di navigazione web e applicazioni in tempo reale, dove la rapidità di stabilimento delle connessioni è fondamentale per la fluidità e la reattività dell'interazione con l'utente.

In sintesi, l'integrazione della crittografia in QUIC rappresenta un avanzamento significativo nella progettazione dei protocolli di rete, mettendo la sicurezza e la privacy al centro dell'esperienza online. Attraverso questo approccio innovativo, QUIC non solo eleva il livello di protezione per gli utenti di Internet ma stabilisce anche un nuovo standard per la sicurezza, l'efficienza e la facilità d'uso nelle comunicazioni digitali.[JI21a]

Controllo della Congestione e Gestione della Perdita di Pacchetti

Il modo in cui QUIC controlla il traffico e gestisce la perdita di dati è come un upgrade rispetto al vecchio TCP mostrando una più profonda comprensione dei problemi delle reti internet di oggi. In un contesto in cui le applicazioni richiedono trasmissioni dati sempre più rapide e affidabili, la capacità di QUIC di gestire in modo efficiente la congestione di rete e le inevitabili perdite di pacchetti diventa molto importaante per mantenere alte prestazioni e una buona esperienza utente.

A differenza di TCP, che tratta la congestione e la perdita di pacchetti attraverso algoritmi uniformi applicati a tutti i flussi di dati all'interno di una connessione, QUIC introduce un approccio più granulare e adattivo. Questo approccio permette a QUIC di reagire alle condizioni di rete in tempo reale, adattando dinamicamente le sue strategie di trasmissione per ottimizzare la consegna dei dati senza sovraccaricare la rete. Tale flessibilità porta ad una riduzione degli effetti negativi della congestione, migliorando la qualità della connessione anche in scenari di rete altamente variabili.

La gestione della perdita di pacchetti in QUIC è altrettanto avanzata. Sfruttando algoritmi di rilevamento delle perdite sofisticati e meccanismi di ritrasmissione selettiva, QUIC è in grado di identificare rapidamente i pacchetti persi e di decidere in modo intelligente quali dati ritrasmettere e quando. Questo non solo riduce la latenza introdotta dalle ritrasmissioni ma minimizza anche l'overhead complessivo della rete, ottimizzando l'uso della banda disponibile.

Un'altro aspetto importante che distingue QUIC nella gestione della congestione e della perdita di pacchetti è la sua capacità di trattare separatamente i diversi flussi di dati multiplexati all'interno della stessa connessione. Questo significa che la perdita di pacchetti in un flusso non rallenta o blocca la trasmissione degli altri flussi, un vantaggio importante rispetto al comportamento di TCP, dove una singola perdita può avere effetti a cascata su tutti i dati in attesa di trasmissione. Grazie a questa indipendenza dei flussi, QUIC migliora notevolmente l'efficienza del trasporto dei dati, garantendo che le applicazioni possano continuare a operare in modo fluido anche di fronte a problemi di rete.

Inoltre, QUIC implementa un sistema di feedback continuo tra il client e il server, facendo si che ci sia un aggiustamento dinamico dei parametri di controllo della congestione in base alle condizioni di rete percepite. Questo dialogo costante aiuta a prevenire situazioni di congestione prima che si verifichino e a reagire prontamente quando sono inevitabili, mantenendo così un flusso di dati costante e affidabile.

Attraverso questi meccanismi avanzati, QUIC non solo affronta alcune delle sfide più pressanti nelle comunicazioni su Internet ma stabilisce anche un nuovo standard per l'efficienza, l'affidabilità e la reattività delle connessioni online. [JI21a]

Estensibilità e Supporto per le Applicazioni

L'estendibilità e il supporto per le applicazioni sono caratteristiche fondamentali che distinguono QUIC dagli altri protocolli di rete. La progettazione di QUIC con un occhio attento all'estendibilità garantisce che il protocollo possa essere adattato e migliorato nel tempo, senza compromettere la compatibilità con le implementazioni esistenti o far fare grossi lavori alla rete. Questo approccio di previsione alla progettazione del protocollo assicura che QUIC non solo soddisfi le esigenze attuali ma sia anche preparato a evolversi in risposta alle future innovazioni tecnologiche e ai cambiamenti nel panorama digitale.

Componente	Caratteristiche
Handshake Efficiente e Connessioni	Processo di negoziazione rapida e ottimizzata
	Riduzione del numero di round-trip per stabilire una connessione
	Supporto per handshake zero-RTT per connessioni più veloci
Crittografia Integrata	Utilizzo di crittografia avanzata per la sicurezza delle comunicazioni
	Protezione dei dati tramite crittografia end-to-end
	Supporto per TLS 1.3 per una sicurezza ottimizzata
Controllo della congestione e Gestione della perdita dei pacchetti	Algoritmi dinamici per adattare il flusso di dati
	Monitoraggio e controllo della congestione per mantenere un flusso di dati stabile e ottimale
	Gestione efficace della perdita di pacchetti per garantire una trasmissione affidabile
Estendibilità e supporto per le applicazioni	Flessibilità per adattarsi a nuove tecnologie e requisiti
	Capacità di estendere il protocollo per nuove funzionalità
	Supporto per diverse applicazioni e scenari di utilizzo

Tabella 3.1: Tabella riassuntiva struttura Generale e componenti di QUIC

Uno degli aspetti chiave dell'estendibilità di QUIC è la sua architettura modulare, che consente l'introduzione di nuove funzionalità, algoritmi di controllo della congestione, meccanismi di sicurezza e ottimizzazioni delle prestazioni attraverso l'aggiunta o la modifica di estensioni al protocollo. Questa flessibilità fa si che QUIC piaccia particolarmente agli sviluppatori e agli operatori di rete, che possono personalizzare e ottimizzare il comportamento del protocollo per meglio adattarsi alle specifiche esigenze delle loro applicazioni e reti, promuovendo l'innovazione e il miglioramento continuo delle prestazioni di rete.

Parallelamente all'estendibilità, QUIC offre un supporto robusto per le applicazioni, evidenziato in modo più elevato dalla sua stretta integrazione con il protocollo HTTP/3. Questo collegamento tra QUIC e HTTP/3 apre nuove frontiere per lo sviluppo di applicazioni web, sfruttando la bassa latenza, il multiplexing senza blocco di testa di linea e la resilienza alle variazioni delle condizioni di rete offerte da QUIC. Gli sviluppatori possono così costruire applicazioni web più reattive e affidabili, che rispondono rapidamente alle interazioni degli utenti e offrono un'esperienza utente fluida e senza interruzioni.[Cor]

L'utilizzo di QUIC come strato di trasporto di base per HTTP/3 sottolinea anche l'impegno del protocollo nel supportare le esigenze di comunicazione delle applicazioni moderne, facilitando uno scambio di dati più efficiente e sicuro su Internet. La combinazione di QUIC con HTTP/3 migliora significativamente le prestazioni delle applicazioni web rispetto a HTTP/2 su TCP, soprattutto in termini di velocità di caricamento delle pagine, efficienza della trasmissione dei dati e resilienza alle perdite di pacchetti e alla latenza di rete.

Attraverso il suo design innovativo e la sua stretta integrazione con protocolli applicativi chiave come HTTP/3, QUIC si posiziona come un elemento trasformativo nel panorama dei protocolli di rete, pronto ad affrontare le sfide del presente e ad adattarsi alle opportunità del futuro.[MP20]

3.2 Flusso dei dati e il concetto di Multiplexing

Il flusso dei dati e il concetto di multiplexing sono elementi centrali nella progettazione e nell'implementazione di protocolli di rete moderni, avendo un ruolo fondamentale nell'ottimizzazione delle prestazioni delle comunicazioni digitali e nell'esperienza utente sul web. Questi concetti sono particolarmente rilevanti nel contesto di QUIC, un protocollo che ha rivoluzionato il modo in cui i dati vengono trasmessi su Internet, offrendo un'alternativa più veloce, sicura e affidabile ai tradizionali TCP e UDP.

3.2.1 Flusso dei Dati

Nel contesto delle comunicazioni di rete, il flusso dei dati è una componente che influisce direttamente sull'efficacia e sull'efficienza con cui le informazioni vengono trasmesse attraverso Internet. La gestione ottimale del flusso dei dati è fondamentale non solo per garantire la rapidità e la fluidità delle interazioni online ma anche per assicurare la stabilità e l'affidabilità delle connessioni in ambienti di rete variabili e spesso imprevedibili. Nell'era digitale, dove il volume e la velocità dei dati in circolazione continuano a crescere esponenzialmente, la capacità di gestire efficacemente il flusso dei dati diventa un elemento di distinzione dei protocolli di rete avanzati, come QUIC, che cercano di superare le limitazioni dei predecessori basati su TCP.

La gestione del flusso dei dati in una rete implica numerose sfide tecniche, tra cui la necessità di bilanciare la velocità di trasmissione con la capacità di rete disponibile, prevenire la congestione di rete e minimizzare la perdita di dati, tutto mentre si mantengono basse le latenze. In questo contesto, le strategie tradizionali hanno sempre avuto problemi, specialmente in scenari dove le condizioni di rete cambiano molto o da elevati requisiti di prestazione. Ad esempio, il meccanismo di controllo della congestione di TCP, pur essendo affidabile per molti usi, può diventare una restrizione per applicazioni che richiedono trasmissioni dati ad alta velocità e in tempo reale, a causa dei suoi algoritmi di controllo del flusso che tendono a essere conservativi per evitare la sovraccarico della rete.

QUIC affronta queste sfide introducendo un modello di gestione del flusso dei dati radicalmente migliorato. Integrando la gestione del flusso direttamente nel protocollo e utilizzando UDP come strato di trasporto sottostante, QUIC offre una maggiore flessibilità nella gestione del traffico di dati. Questo approccio permette a QUIC di adattarsi rapidamente alle variazioni delle condizioni di rete, ottimizzando la velocità di trasmissione in base alla capacità disponibile e riducendo il rischio di congestione. Inoltre, QUIC è progettato per rilevare e rispondere alla perdita di pacchetti in modo più efficace rispetto a TCP, utilizzando algoritmi che permettono una più rapida ripresa delle trasmissioni dopo interruzioni, garantendo così che il flusso dei dati rimanga il più possibile ininterrotto.

La gestione avanzata del flusso dei dati in QUIC non solo migliora le prestazioni delle singole connessioni ma ha anche implicazioni positive più ampie sull'intero ecosistema di Internet. Per le applicazioni web, ciò comporta caricamenti di pagina più rapidi, streaming multimediale di migliore qualità e comunicazioni interattive più reattive. Per gli utenti finali, significa un'esperienza online complessivamente migliore, con minori attese e interruzioni. E per gli operatori di rete, significa una maggiore efficienza nella gestione del traffico, con potenziali riduzioni dei costi operativi e miglioramenti nella soddisfazione degli utenti.

Percio, il flusso dei dati in QUIC rappresenta un'evoluzione significativa nella gestione delle comunicazioni digitali, offrendo un modello più dinamico, resiliente e performante rispetto a quelli tradizionali. [FC21]

3.2.2 Concetto di Multiplexing

Il concetto di multiplexing, soprattutto quando applicato al protocollo QUIC, rappresenta una svolta nella gestione efficiente e dinamica dei flussi di dati attraverso le reti. Tradizionalmente, i protocolli come TCP affrontano una serie di limitazioni strutturali che possono influenzare negativamente l'efficienza delle comunicazioni, in particolare il fenomeno noto come blocco di testa di linea (head-of-line blocking), dove la perdita di un singolo pacchetto può ritardare la consegna di tutti i pacchetti successivi in coda. Questo problema si manifesta in modo grave in contesti di rete con alta latenza o elevata perdita di pacchetti, dove anche una singola interruzione può avere un impatto significativo sull'esperienza complessiva dell'utente.

Il multiplexing in QUIC, tuttavia, introduce un approccio radicalmente diverso, consentendo a più flussi di dati di coesistere simultaneamente all'interno della stessa connessione fisica senza interferire l'uno con l'altro. Ciò significa che, anche se un flusso di dati incontra problemi, come la perdita di pacchetti, gli altri flussi possono continuare indisturbati, eliminando efficacemente il problema del blocco di testa di linea e migliorando notevolmente l'efficienza complessiva della trasmissione dei dati.

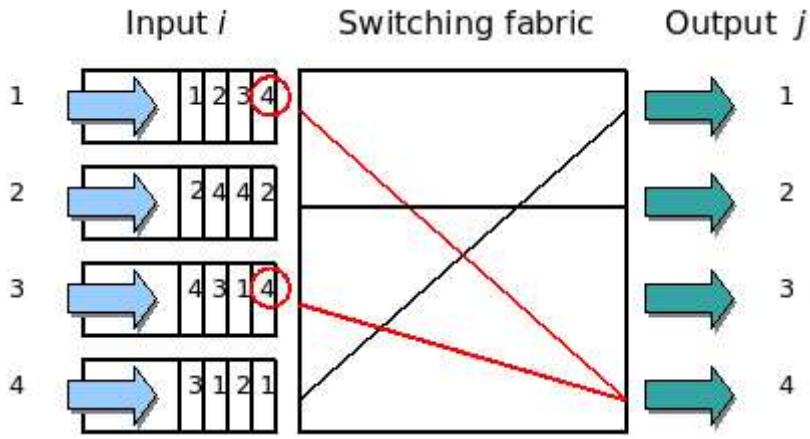

Figura 3.1: Head-of-line-blocking[Imma]

Questo modello di multiplexing offre vantaggi importanti per lo sviluppo e il funzionamento delle applicazioni web moderne, che spesso hanno bisogno di caricare una varietà di risorse — come CSS, JavaScript, immagini e contenuti video — in modo simultaneo. Grazie al multiplexing di QUIC, questi elementi possono essere trasmessi in parallelo su flussi separati, accelerando il caricamento delle pagine web e migliorando l'interattività e la reattività delle applicazioni. Inoltre, la capacità di gestire flussi multipli in maniera indipendente permette una più fine ottimizzazione della larghezza di banda e una migliore adattabilità alle condizioni di rete in continuo cambiamento, garantendo così un'esperienza utente ottimale anche in scenari di rete sfavorevoli.

Un altro aspetto fondamentale del multiplexing in QUIC è la sua estrema flessibilità e scalabilità. Gli sviluppatori possono sfruttare questa caratteristica per costruire applicazioni che si adattano dinamicamente alle esigenze degli utenti e alle condizioni di rete, migliorando il flusso di dati in tempo reale e assicurando la massima efficienza nella consegna dei contenuti. Questo livello di controllo e adattabilità apre nuove possibilità per l'innovazione nelle applicazioni web, permettendo di esplorare nuovi modelli di interazione e di presentazione dei contenuti che erano precedentemente limitati dalle restrizioni dei protocolli di rete tradizionali.

Il multiplexing rappresenta un elemeneto fondamentale della struttura di QUIC, offrendo un metodo più avanzato e flessibile per la gestione dei flussi di dati su Internet. Superando le limitazioni dei protocolli precedenti e abilitando una trasmissione dei dati più efficiente e resiliente, il multiplexing in QUIC non solo migliora l'esperienza utente finale ma spiana anche la strada a una nuova generazione di applicazioni web più ricche, interattive e performanti.[JI21b]

Il flusso dei dati e il concetto di multiplexing sono elementi essenziali per comprendere le moderne comunicazioni digitali e il funzionamento dei protocolli di rete. QUIC, con il suo approccio rivoluzionario al multiplexing e alla gestione del flusso dei dati, rappresenta un passo avanti significativo nella tecnologia di rete, promettendo di rendere Internet un luogo più veloce, sicuro e affidabile per tutti.

3.3 Integrazione di QUIC nel progetto Chromium

L'integrazione del protocollo QUIC nel progetto Chromium ha segnato una svolta significativa nel panorama dei browser web. Chromium, la base open-source su cui è

costruito Google Chrome, ha giocato un ruolo cruciale nell'adozione e nella promozione di QUIC, dimostrando i suoi vantaggi in un ambiente di utilizzo reale e diffuso.

L'adozione di QUIC da parte di Chromium è stata motivata dalla necessità di migliorare le prestazioni di navigazione su internet. QUIC, con le sue caratteristiche di bassa latenza e gestione efficiente del traffico dati, si è dimostrato un'ottima soluzione per accelerare il caricamento delle pagine web e migliorare la reattività delle applicazioni online.

In Chromium, QUIC ha portato miglioramenti tangibili nel tempo di caricamento delle pagine. Grazie alla sua gestione ottimizzata del multiplexing e alla riduzione della latenza nei processi di handshake, QUIC ha permesso una comunicazione più rapida e fluida tra il browser e i server. Questo ha portato a una navigazione più veloce e a un'esperienza utente migliorata, riducendo i tempi di attesa per gli utenti.

L'integrazione di QUIC ha anche rafforzato la sicurezza in Chromium. Essendo un protocollo che integra la crittografia end-to-end, QUIC ha elevato il livello di sicurezza delle connessioni, un aspetto fondamentale nell'uso quotidiano di internet. La crittografia nativa di QUIC assicura che i dati trasmessi siano protetti, contribuendo a una navigazione più sicura e privata.

L'uso di QUIC in Chromium ha avuto un impatto significativo anche sullo sviluppo e la standardizzazione del protocollo a livello globale. L'esperienza acquisita attraverso l'implementazione di QUIC in un browser ampiamente usato come Chrome ha fornito dati preziosi per il suo sviluppo continuo. Questi dati hanno contribuito alla decisione dell'IETF di adottare QUIC come standard, influenzando il modo in cui i dati vengono trasmessi su internet.

Oltre a migliorare le prestazioni di navigazione e la sicurezza, l'integrazione di QUIC in Chromium ha anche offerto vantaggi in termini di affidabilità e stabilità della connessione. QUIC è progettato per essere più resiliente nei confronti di cambiamenti nella rete e perdita di pacchetti, caratteristiche particolarmente utili in ambienti con connessioni internet instabili o di qualità variabile.

In conclusione, l'integrazione di QUIC nel progetto Chromium ha rappresentato non solo un significativo miglioramento tecnologico per il browser, ma ha anche avuto un ruolo fondamentale nell'evoluzione generale dei protocolli di comunicazione su internet. Con l'adozione di QUIC, Chromium ha stabilito nuovi standard di velocità, sicurezza e affidabilità per la navigazione web, influenzando positivamente l'esperienza degli utenti in tutto il mondo.

4. Vantaggi e sfide di QUIC

4.1 Vantaggi di QUIC rispetto a TCP

Il protocollo QUIC (Quick UDP Internet Connections) ha introdotto un'innovazione significativa nel panorama delle comunicazioni su Internet, proponendosi come una valida alternativa al tradizionale TCP (Transmission Control Protocol). Entrambi progettati per affidabilità e ordine nella consegna dei dati, QUIC e TCP si differenziano però in modi che offrono vantaggi distinti, soprattutto in termini di velocità, sicurezza, efficienza della connessione e gestione della congestione. Esaminiamo questi vantaggi in modo più dettagliato, mettendo in luce le differenze tra QUIC e TCP.

4.1.1 Riduzione della Latenza nella Connessione

Uno degli obiettivi primari nella progettazione di QUIC è stato quello di minimizzare la latenza introdotta durante la fase di stabilimento della connessione, un aspetto dove TCP, specialmente quando combinato con TLS per connessioni sicure mostra i suoi limiti.

Handshake TCP + TLS

In una tipica connessione TCP con sicurezza TLS, il processo per stabilire una connessione sicura richiede multiple fasi:

Un handshake a tre fasi per stabilire la connessione TCP. Un successivo handshake TLS per negoziare i parametri di crittografia e scambiare le chiavi, che richiede ulteriori round trip tra client e server. Questo processo può comportare notevoli ritardi prima che possano essere inviati dati utili, specialmente in reti con latenza elevata o in scenari di connessioni mobili, dove la latenza aggiuntiva è particolarmente penalizzante per l'esperienza utente.[Com13]

Handshake QUIC

QUIC, d'altra parte, riduce significativamente questa latenza grazie a un approccio integrato:

Combina la negoziazione della connessione e la negoziazione crittografica in un unico round trip (1-RTT). Per le connessioni a siti già visitati, QUIC può addirittura procedere con 0-RTT, dove i dati vengono inviati immediatamente insieme alla richiesta di riconnessione, utilizzando le chiavi crittografiche precedentemente negoziate. Il supporto per 0-RTT riduce drasticamente il tempo necessario per inviare dati utili, offrendo un vantaggio notevole per applicazioni che richiedono connessioni frequenti e rapide,

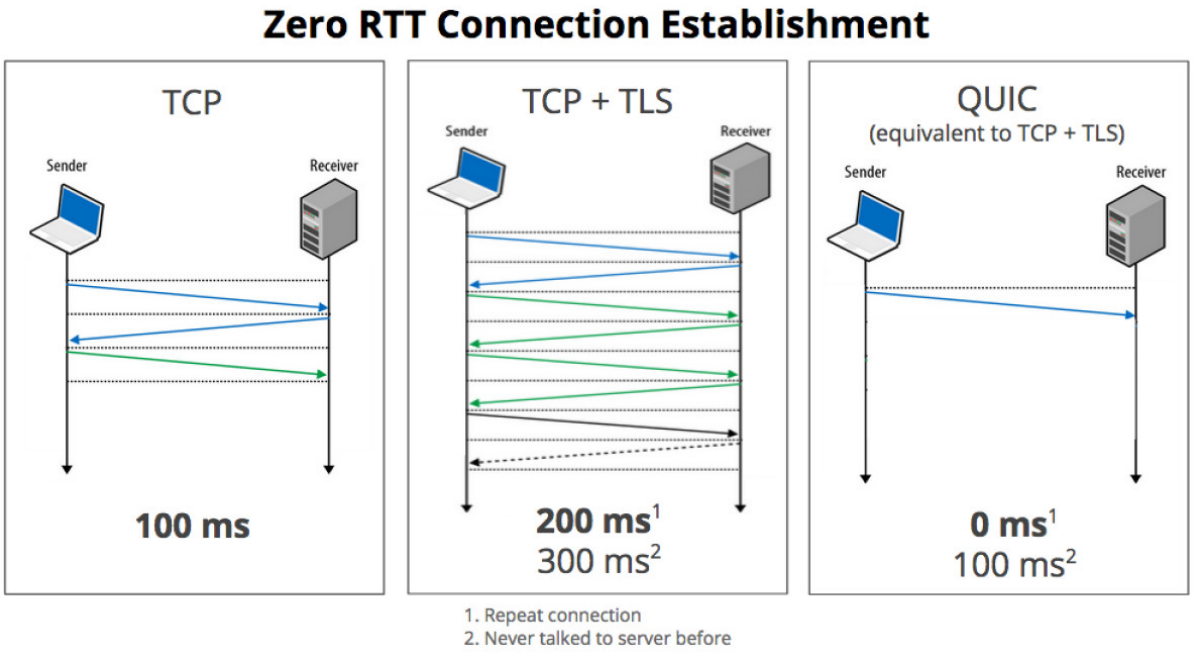

Figura 4.1: [Immb]

come le richieste web in siti di e-commerce, piattaforme di streaming e servizi online che dipendono da interazioni in tempo reale.[JI21a]

Impatto sulla Latenza di Connessione

La riduzione della latenza di connessione ha un impatto diretto sull'esperienza dell'utente:

Le pagine web si caricano più rapidamente, migliorando la percezione della velocità da parte dell'utente e potenzialmente contribuendo a tassi di conversione più elevati per le piattaforme di e-commerce. Le applicazioni di streaming video e audio beneficiano di avvii più veloci dei contenuti, riducendo l'attesa per l'utente. I giochi online e le applicazioni di comunicazione realizzano connessioni più veloci, migliorando la qualità dell'esperienza utente in scenari di mobilità e reti variabili. La capacità di QUIC di ridurre la latenza nella fase di stabilimento della connessione offre un vantaggio competitivo significativo rispetto a TCP, specialmente in un'era dove la velocità e l'efficienza delle connessioni internet sono di fondamentale importanza per un'ampia varietà di applicazioni e servizi online. La combinazione di un handshake efficiente con la crittografia integrata posiziona QUIC come una soluzione avanguardistica per i problemi di latenza e sicurezza nelle comunicazioni su internet.[**quic-http/3**]

4.1.2 Eliminazione del Head-of-Line Blocking

Il head-of-line blocking è un problema noto nelle reti che utilizzano TCP come protocollo di trasporto, in particolare quando si trasmettono dati su connessioni multiplexate come quelle stabilite in HTTP/2 su TCP. In TCP, i dati sono ricevuti e consegnati all'applicazione in ordine. Se un pacchetto viene perso, TCP deve attendere la riconsegna di quel pacchetto prima di poter consegnare tutti i pacchetti successivi alla coda,

anche se sono già stati ricevuti. Questo può causare ritardi significativi, soprattutto in scenari di rete con alta latenza o perdita di pacchetti.[**<empty citation>**]

QUIC e il Multiplexing dei Flussi

QUIC affronta il problema del HOL blocking utilizzando un approccio basato sul multiplexing dei flussi all'interno della stessa connessione UDP. Ogni flusso è essenzialmente indipendente e può essere trasmesso in parallelo senza essere bloccato dai ritardi di altri flussi. Se un pacchetto di un determinato flusso viene perso, solo quel particolare flusso viene influenzato dalla necessità di attendere una riconsegna, mentre gli altri flussi continuano il loro trasferimento senza interruzioni.

Benefici del Multiplexing in QUIC

Riduzione della Latenza per le Applicazioni Web: Proprio come detto poco fa, le applicazioni web che richiedono l'invio simultaneo di molteplici risorse, come file CSS, JavaScript e immagini, QUIC migliora significativamente i tempi di caricamento delle pagine riducendo la latenza causata dal HOL blocking. Miglioramento dell'Esperienza di Streaming: Servizi di streaming video e audio traggono vantaggio dal multiplexing di QUIC, in quanto la perdita di pacchetti in un flusso (ad esempio, un flusso di dati non critici) non rallenta la consegna di altri flussi critici, garantendo una riproduzione più fluida. Affidabilità nelle Connessioni di Gioco Online: Nei giochi online, dove il tempo di reazione e l'aggiornamento costante dello stato di gioco sono cruciali, QUIC può migliorare l'esperienza degli utenti minimizzando i ritardi dovuti alla perdita di pacchetti.

Implementazione Tecnica

QUIC realizza il multiplexing dei flussi gestendo ogni flusso come una sequenza di messaggi indipendenti. La numerazione dei pacchetti e il controllo dell'affidabilità sono gestiti per flusso, consentendo a QUIC di riconoscere e riconsegnare selettivamente i dati mancanti per ciascun flusso senza influenzare gli altri. Questo è reso possibile grazie all'uso di un modello di trasmissione basato su UDP, che, a differenza di TCP, non impone un ordine stretto nella consegna dei pacchetti all'applicazione destinataria.

Eliminando il problema del head-of-line blocking attraverso un'innovativa gestione dei flussi di dati, QUIC offre una soluzione potente per migliorare la velocità, l'affidabilità e l'efficienza delle comunicazioni su internet. La sua capacità di gestire indipendentemente i flussi di dati all'interno di una singola connessione non solo ottimizza la trasmissione dei dati in scenari di uso intensivo ma migliora anche significativamente l'esperienza dell'utente finale in una vasta gamma di applicazioni online.[JI21b]

4.1.3 Sicurezza Integrata

Uno degli aspetti più innovativi di QUIC è l'integrazione nativa della sicurezza nel suo design, contrariamente a TCP, che richiede l'aggiunta di TLS (Transport Layer Security) come strato separato per ottenere comunicazioni crittografate. QUIC incorpora la crittografia end-to-end basata su TLS 1.3 direttamente nel protocollo, assicurando che tutte le informazioni trasmesse siano protette fin dall'inizio della connessione.

Figura 4.2: [Immc]

Crittografia Fin dall'Handshake

Handshake Integrato: QUIC integra l'handshake di TLS 1.3 nel suo processo di stabilimento della connessione, consentendo la negoziazione dei parametri crittografici e lo scambio delle chiavi contemporaneamente all'apertura della connessione. Questo riduce i round trip necessari per iniziare la trasmissione sicura dei dati e minimizza la latenza. 0-RTT e 1-RTT: Grazie all'handshake ottimizzato e alla possibilità di riutilizzare le informazioni di sessione precedenti, QUIC supporta la connessione 0-RTT, permettendo ai dati di essere trasmessi in modo sicuro con zero round trip aggiuntivi nelle connessioni successive, un vantaggio significativo per le prestazioni senza compromettere la sicurezza.

Miglioramenti della Sicurezza Rispetto a TCP+TLS

Protezione contro Attacchi di Downgrade: QUIC prevede meccanismi specifici per proteggersi contro gli attacchi di downgrade, impedendo agli aggressori di costringere la connessione a utilizzare versioni meno sicure del protocollo o cifrature più deboli. Confidenzialità del Numero di Sequenza: A differenza di TCP, dove i numeri di sequenza sono trasmessi in chiaro, in QUIC anche i numeri di pacchetto sono crittografati, rendendo più difficile per gli osservatori esterni tracciare o manipolare specifici pacchetti all'interno di una connessione. Indipendenza dal Layer di Rete: Dato che QUIC è implementato sopra UDP e gestisce internamente le funzionalità di affidabilità e sicurezza, è meno suscettibile alle problematiche di sicurezza che possono affliggere il layer di rete, offrendo una maggiore protezione contro gli attacchi basati su IP spoofing o route hijacking.

Benefici per gli Sviluppatori e gli Utenti

Semplicità di Implementazione: Integrando la sicurezza direttamente, QUIC semplifica lo stack di rete per gli sviluppatori di applicazioni, riducendo la complessità e il sovraccarico associati alla gestione separata di TLS su TCP. Maggiore Privacy e Sicurezza per gli Utenti: La crittografia end-to-end di QUIC non solo protegge i dati trasferiti ma anche i metadati sensibili, come i pattern di traffico e la dimensione dei pacchetti, migliorando la privacy degli utenti.

La sicurezza integrata di QUIC rappresenta un passo avanti significativo nella protezione delle comunicazioni su Internet. Offrendo vantaggi come la riduzione della latenza nella fase di handshake, una maggiore protezione contro gli attacchi e una semplificazione dell'implementazione per gli sviluppatori, QUIC stabilisce nuovi standard di sicurezza e prestazioni per le applicazioni online. Con la sua adozione crescente, QUIC si prospetta come il futuro delle comunicazioni sicure su Internet, promettendo un web più veloce, più sicuro e più affidabile per tutti gli utenti.[MT21]

4.1.4 Migliore Gestione della Congestione e del Recupero delle Perdite

QUIC introduce miglioramenti significativi nella gestione della congestione e nel recupero delle perdite rispetto a TCP, sfruttando algoritmi avanzati e un approccio più

granulare per ottimizzare il traffico di rete e ridurre l'impatto delle perdite di pacchetti.

Gestione della Congestione in QUIC

Approccio Basato su Feedback: QUIC utilizza un modello di feedback esplicito per la gestione della congestione, ricevendo conferme di ricezione (ACK) per pacchetti specifici e adattando dinamicamente la velocità di invio in base alle condizioni attuali della rete. Questo consente a QUIC di reagire rapidamente alle variazioni di latenza e disponibilità della banda, migliorando l'efficienza del throughput. Algoritmi di Congestione Personalizzabili: A differenza di TCP, dove la scelta degli algoritmi di controllo della congestione è spesso limitata dal sistema operativo, QUIC permette l'implementazione e la sperimentazione di diversi algoritmi direttamente nello spazio utente. Questa flessibilità favorisce l'adozione di strategie ottimizzate per specifici scenari di applicazione o condizioni di rete.

Recupero delle Perdite

Rilevamento e Recupero Rapido: QUIC migliora il recupero delle perdite implementando tecniche come il rilevamento delle perdite basato sul tempo, che consente di identificare e ritrasmettere rapidamente i pacchetti persi senza dover attendere timeout prolungati. Questo riduce significativamente il tempo necessario per ripristinare la trasmissione efficace dopo interruzioni. Forward Error Correction (FEC): Alcune implementazioni di QUIC possono includere meccanismi di Forward Error Correction per recuperare i dati persi senza la necessità di ritrasmissioni, aumentando ulteriormente la resilienza alle condizioni di rete avverse.

Impatto sulla Qualità dell'Esperienza

Streaming Video e Audio: Per le applicazioni di streaming, una gestione della congestione e un recupero delle perdite più efficaci significano meno interruzioni e una qualità di riproduzione migliore, anche su reti congestionate o instabili. Applicazioni Interattive: Giochi online, videoconferenze e altre applicazioni interattive beneficiano enormemente della ridotta latenza e della maggiore reattività offerte dalla gestione avanzata della congestione e dal recupero rapido delle perdite in QUIC, risultando in un'esperienza utente più fluida e coinvolgente.

La gestione avanzata della congestione e il recupero delle perdite in QUIC rappresentano un salto qualitativo rispetto alle tecniche impiegate in TCP. Attraverso l'uso di feedback esplicito, algoritmi personalizzabili, e tecniche innovative di rilevamento e recupero delle perdite, QUIC è in grado di ottimizzare l'uso della banda disponibile, ridurre la latenza e migliorare l'affidabilità delle connessioni. Questi miglioramenti si traducono in un'esperienza utente notevolmente superiore per una vasta gamma di applicazioni Internet, dalla navigazione web allo streaming di contenuti multimediali, rendendo QUIC una tecnologia chiave per il futuro delle comunicazioni su Internet[JI21a]

4.1.5 Mobilità

La mobilità è uno degli aspetti in cui QUIC supera significativamente TCP, grazie alla sua progettazione orientata a soddisfare le esigenze degli utenti in movimento. In un mondo sempre più connesso, dove passare da una rete all'altra è comune, la capacità di mantenere sessioni stabili e performanti durante i cambi di rete è fondamentale.

Identificatori di Connessione

Connessioni Resilienti: QUIC introduce gli identificatori di connessione (Connection ID), che permettono alle sessioni di persistere nonostante i cambiamenti nell'indirizzo IP o nella porta del client. Questo è particolarmente utile per dispositivi mobili che passano frequentemente tra reti cellulari e Wi-Fi, assicurando che le applicazioni mantengano una connessione continua senza necessità di ristabilire sessioni. Supporto alla Mobilità senza Interruzioni: Gli identificatori di connessione consentono a QUIC di gestire le transizioni di rete in modo trasparente, riducendo significativamente la latenza e i potenziali timeout che possono verificarsi con TCP quando si verifica un cambio di rete.

4.1.6 Miglioramenti nella User Experience

Navigazione Web Continua: Per la navigazione web, QUIC garantisce che le pagine e le risorse continuino a caricarsi senza interruzioni mentre un utente si muove, migliorando l'esperienza generale di utilizzo di Internet su dispositivi mobili. Streaming Senza Interruzioni: Per lo streaming di contenuti video o audio, QUIC minimizza gli effetti dei cambi di rete, assicurando una riproduzione fluida e senza interruzioni, critica per mantenere elevata la soddisfazione dell'utente.

Vantaggi per gli Sviluppatori di Applicazioni

Semplificazione della Gestione dello Stato: Per gli sviluppatori, QUIC riduce la complessità nel gestire i cambi di stato della rete nelle loro applicazioni, poiché la resilienza alle variazioni dell'indirizzo è gestita a livello di protocollo. Opportunità di Innovazione: La stabilità migliorata delle connessioni in scenari di mobilità apre nuove possibilità per lo sviluppo di applicazioni mobili innovative, particolarmente quelle che richiedono connettività costante e bassa latenza, come i giochi online multiplayer, applicazioni di realtà aumentata e servizi di localizzazione in tempo reale.

La mobilità migliorata è uno dei vantaggi distintivi di QUIC, offrendo una soluzione robusta e efficiente per le sfide poste da un ambiente Internet sempre più mobile e dinamico. Attraverso l'uso di identificatori di connessione unici e la gestione integrata dei cambi di rete, QUIC si posiziona come il protocollo di trasporto ideale per l'era moderna, dove utenti e dispositivi sono costantemente in movimento. La resilienza e l'efficienza di QUIC in scenari di mobilità non solo migliorano l'esperienza dell'utente finale ma anche semplificano lo sviluppo e la manutenzione di applicazioni mobili, promuovendo un'adozione più ampia di questo protocollo innovativo.[Ahm16]

4.1.7 Efficienza nell'Uso del Protocollo UDP per QUIC

Il protocollo QUIC, adottando UDP (User Datagram Protocol) come suo strato di trasporto di base, introduce un miglioramento significativo in termini di efficienza rispetto ai tradizionali protocolli basati su TCP. Questa decisione porta con sé vari vantaggi che si riflettono direttamente sulle prestazioni delle applicazioni web e sui servizi online.

Riduzione dell'Overhead di Protocollo

Overhead Minimizzato: UDP ha un overhead di intestazione molto più ridotto rispetto a TCP, risultando in un maggiore payload utile per pacchetto e quindi in una mag-

	TCP	UDP
Structure	Segments	Datagrams
Connection Model	Connected, one-to-one	Connectionless, one-to-many
Data Transfer	Ordered	Unordered
Reliability	Reliable	Unreliable
Overhead	Resource intensive	Lightweight

Figura 4.3: [Ult]

giore efficienza di banda. Questo è particolarmente vantaggioso per le applicazioni che richiedono tempi di risposta rapidi e un alto throughput.

Controllo e Flessibilità Migliorati

Gestione Personalizzata: Essendo QUIC implementato su UDP, può includere la propria logica per la riconsegna di pacchetti, controllo della congestione, e gestione della sessione, consentendo un'ottimizzazione specifica per le esigenze delle applicazioni che lo utilizzano. Questo offre agli sviluppatori un controllo granulare senza precedenti sul comportamento della trasmissione dati. Agilità nello Sviluppo: Operando nello spazio utente, QUIC permette un ciclo di sviluppo e distribuzione più rapido per nuove funzionalità e miglioramenti, indipendentemente dai vincoli dei sistemi operativi o dei dispositivi.

Miglioramento delle Prestazioni

Avvio Rapido delle Connessioni: Grazie alla combinazione di handshake ridotti e alla capacità di bypassare la lenta avviatura (slow start) di TCP, QUIC su UDP può iniziare a trasmettere dati significativi quasi immediatamente dopo l'avvio di una connessione. Questo è vitale per migliorare l'esperienza utente in applicazioni web dinamiche e servizi di streaming. Risposta alle Fluttuazioni della Rete: La gestione indipendente della congestione e del controllo degli errori consente a QUIC di adattarsi rapidamente ai cambiamenti nelle condizioni della rete, mantenendo prestazioni ottimali anche in ambienti altamente variabili.

Sfide e Considerazioni

Nonostante i vantaggi, l'uso di UDP comporta alcune considerazioni. Le reti e i dispositivi configurati strettamente per ottimizzare o filtrare il traffico TCP possono richiedere aggiornamenti per supportare efficacemente QUIC. Inoltre, gli sviluppatori devono considerare la gestione della qualità del servizio (QoS) e la potenziale necessità di negoziare con operatori di rete e fornitori di infrastrutture per garantire che il traffico UDP non venga indebitamente limitato o bloccato.[JI21b]

L'efficienza nell'uso del protocollo UDP da parte di QUIC rappresenta un cambio di paradigma nelle comunicazioni di rete, offrendo una piattaforma per applicazioni

Riduzione della latenza nella connessione	QUIC minimizza la latenza di stabilimento della connessione attraverso un handshake ottimizzato, incluso il supporto per 0-RTT nelle connessioni già stabilite.
Eliminazione del Head-of-Line Blocking	QUIC affronta il problema del HOL blocking grazie al multiplexing dei flussi all'interno della stessa connessione UDP.
Sicurezza integrata	QUIC incorpora la crittografia end-to-end basata su TLS 1.3 direttamente nel protocollo, garantendo che tutte le informazioni trasmesse siano protette fin dall'inizio della connessione.
Migliore gestione della congestione e del recupero delle perdite	QUIC introduce miglioramenti significativi nella gestione della congestione e nel recupero delle perdite attraverso l'uso di algoritmi avanzati e un approccio più granulare.
Mobilità	QUIC supera significativamente TCP grazie agli identificatori di connessione, consentendo sessioni stabili e performanti durante i cambiamenti di rete.
Efficienza nell'uso del protocollo UDP	QUIC, utilizzando UDP come base, offre un overhead di protocollo ridotto e una maggiore flessibilità nella gestione personalizzata.

Tabella 4.1: Tabella riassuntiva dei vantaggi di QUIC rispetto a TCP

Internet più reattive, affidabili e performanti. Mentre le sfide nell'adozione e nella compatibilità di rete persistono, i vantaggi in termini di prestazioni e flessibilità di sviluppo posizionano QUIC come una tecnologia chiave per il futuro delle comunicazioni digitali.

4.2 Possibili sfide e problematiche

Il protocollo QUIC (Quick UDP Internet Connections) è stato progettato per superare molte delle limitazioni dei protocolli esistenti come TCP, offrendo miglioramenti significativi in termini di velocità, sicurezza e affidabilità delle connessioni Internet. Tuttavia, nonostante i suoi numerosi vantaggi, QUIC affronta diverse sfide e problematiche che potrebbero influenzarne l'adozione e l'efficacia. Esploriamo queste sfide in modo dettagliato.

4.2.1 Sfide di Compatibilità e Interoperabilità

Progettato per migliorare le prestazioni complessive delle comunicazioni su Internet, QUIC si basa su UDP, un'alternativa a TCP che è stato per lungo tempo il pilastro delle trasmissioni di dati online. Questa scelta fondamentale, sebbene porti con sé numerosi vantaggi in termini di efficienza e flessibilità, introduce complessità in termini di interazione con la vasta gamma di dispositivi di rete e software esistenti che sono stati ottimizzati per operare principalmente con TCP.

La sfida principale risiede nel fatto che molti dispositivi di sicurezza di rete, come firewall e sistemi di prevenzione delle intrusioni, così come i dispositivi di Network Address Translation (NAT), hanno regole e configurazioni molto profonde che presuppongono o favoriscono esplicitamente il traffico TCP. Questo orientamento storico verso TCP può portare a delle situazioni dove il traffico QUIC viene erroneamente bloccato o fortemente limitato, compromettendo la connettività e le prestazioni delle applicazioni che si affidano a questo protocollo per una trasmissione dati efficiente e sicura. Per superare questo problema c'è bisogno non solo di un aggiornamento tecnologico ma anche un cambiamento di mentalità tra coloro che gestiscono l'infrastruttura di rete, affinché riconoscano il valore e l'importanza di supportare protocolli basati su UDP come QUIC.

Inoltre, l'adozione di QUIC implica la necessità di aggiornare, riconfigurare o sostituire l'hardware di rete esistente per garantire compatibilità totale con il protocollo. Questo processo può essere particolarmente difficile per le grandi organizzazioni o per i fornitori di servizi Internet che dispongono di infrastrutture complesse e distribuite su larga scala. La transizione verso un supporto efficace di QUIC richiede grossi investimenti in termini di tempo, risorse finanziarie e sforzi di formazione, dato che il personale IT deve acquisire familiarità con le specificità del protocollo e le best practice per la sua implementazione e manutenzione.

La questione dell'interoperabilità si estende anche al modo in cui QUIC interagisce con altre tecnologie di ottimizzazione della rete, come le Content Delivery Networks (CDN) e i proxy di accelerazione web. Mentre queste tecnologie sono fondamentali per migliorare l'accessibilità e le prestazioni dei contenuti online, devono essere attentamente adattate per lavorare in modo efficiente con QUIC, facendo si che le ottimizzazioni implementate non compromettano le caratteristiche distintive del protocollo, come la riduzione della latenza e la sicurezza migliorata.

Affrontare le sfide di compatibilità e interoperabilità di QUIC richiede un approccio coordinato che coinvolga sviluppatori, operatori di rete, fornitori di hardware e software, e organismi di standardizzazione.

4.2.2 Gestione della Congestione e del Controllo delle Perdite

La gestione della congestione e il controllo delle perdite determinano l'efficacia e l'efficienza di qualsiasi protocollo di trasporto su Internet, e QUIC introduce approcci innovativi per affrontare entrambe queste sfide in maniera più sofisticata rispetto a quanto fatto da TCP. L'architettura di QUIC, progettata per operare su UDP, permette non solo di ridurre la latenza attraverso l'eliminazione del cosiddetto "head-of-line blocking", ma anche di implementare meccanismi avanzati per la gestione della congestione e il recupero delle perdite, mirati a ottimizzare le prestazioni di rete anche in condizioni di elevata variabilità.

Nel cuore di QUIC vi è un sistema di feedback che permette una gestione della congestione altamente reattiva e dinamica. Diversamente da TCP, che si affida principalmente su algoritmi di controllo della congestione come Reno o Cubic, che aumentano o diminuiscono la finestra di congestione basandosi su perdite di pacchetti o su segnali di Round-Trip Time (RTT), QUIC utilizza ack dei pacchetti per regolare il flusso di dati in modo più granulare. Questo approccio consente a QUIC di adattarsi rapidamente alle condizioni di rete in cambiamento, migliorando l'utilizzo della banda e riducendo i tempi di attesa per il recupero dei dati persi.

Il controllo delle perdite in QUIC è altrettanto avanzato. Mentre TCP si affida a timer di ritrasmissione per identificare le perdite, spesso portando a ritardi prima che i dati possano essere ritrasmessi, QUIC implementa meccanismi di rilevamento delle perdite basati sia sul tempo che sull'ordine di arrivo dei pacchetti. Questo permette a QUIC di identificare e ritrasmettere rapidamente i pacchetti persi, migliorando significativamente l'efficienza della trasmissione. Inoltre, QUIC è in grado di distinguere tra perdite di pacchetti causate da congestione della rete e ritardi temporanei, permettendo di migliorare ulteriormente il controllo della congestione e di evitare riduzioni inutili della velocità di trasmissione.

Un'altra innovazione chiave di QUIC nel contesto della gestione della congestione e del controllo delle perdite è la sua capacità di supportare il multiplexing di più flussi di dati all'interno di una singola connessione senza incorrere nel head-of-line blocking. Questo significa che la perdita di pacchetti in un singolo flusso di dati non rallenta la trasmissione degli altri flussi, consentendo una maggiore efficienza complessiva e una migliore esperienza per l'utente finale.

Tuttavia, l'implementazione efficace di questi meccanismi avanzati non è priva di sfide. La necessità di bilanciare la rapidità del recupero delle perdite con la prevenzione della congestione della rete richiede un tuning fine e un'attenta considerazione delle dinamiche di rete specifiche. Inoltre, la varietà di ambienti di rete in cui QUIC deve operare, da connessioni mobili ad alta latenza a reti cablate ad alta velocità, pone ulteriori difficoltà nella progettazione di algoritmi universali che possano funzionare in modo ottimale in tutti questi contesti.

Nonostante queste sfide, l'approccio innovativo di QUIC alla gestione della congestione e al controllo delle perdite rappresenta un passo importante verso il miglioramento delle prestazioni e dell'affidabilità delle comunicazioni su Internet. Attraverso un continuo sviluppo e l'adattamento degli algoritmi in base ai feedback della rete e alle ricerche nel campo, QUIC è ben posizionato per affrontare le sfide del trasporto di dati su Internet oggi e in futuro.[JI21a]

4.2.3 Prestazioni e Ottimizzazione

Le prestazioni e l'ottimizzazione di QUIC rappresentano un ambito di particolare interesse e sfida, poiché questo protocollo promette di rivoluzionare il modo in cui dati e informazioni vengono trasferiti su Internet. Hanno un ruolo fondamentale nella filosofia di QUIC la riduzione della latenza, l'aumento della velocità di trasmissione e una migliore affidabilità complessiva rispetto a TCP, sfruttando UDP come strato di trasporto. Tuttavia, realizzare queste promesse implica affrontare e superare diverse sfide tecniche e pratiche.

Il miglioramento delle prestazioni attraverso QUIC si concentra innanzitutto sulla sua capacità di stabilire connessioni più rapidamente, grazie alla riduzione dei round trip necessari per l'handshake iniziale e alla possibilità di riprendere sessioni precedenti quasi istantaneamente con il meccanismo 0-RTT. Questo aspetto è particolarmente vantaggioso per le applicazioni web dinamiche e i servizi che dipendono da frequenti nuove connessioni, come le richieste HTTP per il caricamento di pagine web. Tuttavia, ottimizzare questi processi per garantire che siano sia veloci che sicuri, specialmente considerando i potenziali rischi di sicurezza legati a replay attacks nelle connessioni 0-RTT, richiede una progettazione attenta e meccanismi di protezione robusti.

In aggiunta, QUIC affronta la sfida di gestire efficacemente la congestione di rete e il controllo delle perdite in maniera più dinamica e reattiva rispetto a TCP. Sebbene i

suoi algoritmi avanzati promettano di adattarsi rapidamente alle condizioni di rete in cambiamento, garantendo flussi di dati costanti e riducendo le interruzioni, l'efficacia di tali algoritmi deve essere continuamente testata e affinata attraverso diverse condizioni di rete e scenari d'uso. Questo implica un processo di ottimizzazione costante, dove feedback reali e simulazioni di rete giocano un ruolo cruciale nell'identificare e risolvere i punti deboli.

Un'altra dimensione critica delle prestazioni di QUIC è legata alla sua interazione con le tecnologie di rete esistenti, come le Content Delivery Networks (CDN) e i sistemi di cache. Integrare efficacemente QUIC in queste architetture, ottimizzandolo per lavorare in sinergia con esse, è fondamentale per realizzare miglioramenti tangibili nella velocità di accesso ai contenuti e nella riduzione della latenza per l'utente finale. Questo richiede non solo adeguamenti tecnici ma anche collaborazioni strategiche tra fornitori di contenuti, sviluppatori di protocolli e provider di infrastrutture di rete.[MG21]

Infine, l'ottimizzazione delle prestazioni di QUIC non si limita solo agli aspetti tecnici ma include anche la considerazione dell'esperienza utente. La capacità di QUIC di migliorare significativamente l'affidabilità e la velocità delle connessioni Internet ha il potenziale di trasformare l'esperienza online, rendendo le interazioni digitali più fluide e soddisfacenti. Tuttavia, realizzare questo potenziale su scala globale richiede un impegno collettivo verso l'innovazione continua, l'adozione diffusa e l'adattamento alle esigenze in evoluzione degli utenti e delle applicazioni Internet.

4.2.4 Interazione con le Tecnologie Esistenti

L'interazione di QUIC con le tecnologie di rete esistenti rappresenta un'area cruciale che influisce sulla sua efficacia e sulla sua capacità di essere adottato su larga scala. Questa sfida non riguarda solo la compatibilità tecnica, ma anche l'integrazione strategica con un'ampia gamma di infrastrutture e servizi che costituiscono l'ecosistema di Internet. Le Content Delivery Networks (CDN), i proxy, i bilanciatori di carico e le reti di distribuzione dei contenuti sono solo alcuni esempi di componenti di rete che devono interagire in modo corretto con QUIC per sfruttare appieno i suoi vantaggi in termini di prestazioni e sicurezza.[MG21]

Le CDN, in particolare, svolgono un ruolo fondamentale nell'ottimizzazione della consegna dei contenuti su Internet, riducendo la latenza e migliorando l'esperienza dell'utente finale. L'integrazione efficace di QUIC in queste reti richiede non solo aggiornamenti tecnici per supportare il nuovo protocollo, ma anche un'attenta considerazione su come le caratteristiche uniche di QUIC, come la crittografia end-to-end e il controllo di congestione avanzato, possono essere sfruttate per migliorare ulteriormente la distribuzione dei contenuti. Ciò implica una collaborazione stretta tra i fornitori di CDN e gli sviluppatori di QUIC per garantire che le ottimizzazioni implementate non compromettano le funzionalità chiave del protocollo.

Allo stesso modo, i bilanciatori di carico e i proxy, che fungono da intermediari nelle comunicazioni di rete, devono essere adattati per gestire efficacemente il traffico QUIC. Questo può includere la capacità di mantenere lo stato delle connessioni QUIC attraverso i loro identificatori unici, gestire correttamente le sessioni 0-RTT e supportare la negoziazione di versione del protocollo. Queste modifiche richiedono un approccio olistico alla progettazione e alla manutenzione di queste tecnologie, assicurando che le prestazioni e la sicurezza non siano compromesse dall'introduzione di QUIC.

Inoltre, l'adozione di QUIC presenta opportunità per riconsiderare e ottimizzare le strategie di sicurezza di rete. Gli strumenti di monitoraggio e analisi del traffico,

ad esempio, devono evolvere per accogliere la natura crittografata del traffico QUIC, sviluppando nuove tecniche per l'ispezione e la gestione del traffico che rispettino la privacy dell'utente e l'integrità dei dati. Questo aspetto sottolinea l'importanza di un dialogo continuo tra la comunità di sicurezza di rete e gli sviluppatori di QUIC, per bilanciare efficacemente le esigenze di sicurezza, privacy e prestazioni.

4.2.5 Conclusione

In conclusione, mentre QUIC promette di trasformare il panorama delle comunicazioni su Internet, le sfide legate alla sua compatibilità, gestione della congestione, sicurezza, prestazioni e interoperabilità con le tecnologie esistenti richiedono una soluzione completa e collaborativa da parte della comunità Internet globale. Superare queste sfide richiederà sforzi congiunti, innovazione e un impegno costante per ottimizzare e

5. Sicurezza in QUIC e The Chromium Project

5.1 Principi di sicurezza in QUIC

Nel contesto del protocollo QUIC, la sicurezza è un principio fondamentale che tocca ogni aspetto della sua progettazione e implementazione. Google ha sviluppato QUIC con l'obiettivo di rendere più sicura e affidabile la comunicazione su Internet, garantendo la protezione dei dati degli utenti e la resistenza alle minacce di sicurezza. Per comprendere appieno i principi di sicurezza di QUIC, è necessario esaminare diversi aspetti chiave del protocollo.

5.1.1 Crittografia End-to-End

La crittografia end-to-end rappresenta uno dei pilastri fondamentali della sicurezza nel protocollo QUIC, garantendo la protezione dei dati durante la loro trasmissione tra il client e il server su Internet. Questo approccio crittografico assicura che i dati siano protetti da eventuali intercettazioni o manipolazioni da parte di terzi non autorizzati lungo il percorso della comunicazione. Vediamo più nel dettaglio come la crittografia end-to-end è implementata e quali sono le sue implicazioni per la sicurezza delle comunicazioni su QUIC.

Il protocollo QUIC utilizza una combinazione di crittografia asimmetrica e simmetrica per garantire la sicurezza delle comunicazioni end-to-end. Quando un client stabilisce una connessione con un server utilizzando QUIC, avviene uno scambio di chiavi crittografiche che vengono utilizzate per proteggere i dati trasmessi tra le due parti. Questo scambio di chiavi avviene in modo sicuro e affidabile, utilizzando algoritmi crittografici moderni e sicuri come l'Ephemeral Diffie-Hellman per generare una chiave condivisa tra il client e il server.

Una volta stabilita la connessione e condivise le chiavi crittografiche, QUIC utilizza la crittografia simmetrica per crittografare e decriptare i dati trasmessi tra il client e il server. Questo significa che entrambe le parti utilizzano la stessa chiave segreta per cifrare e decifrare i dati durante la comunicazione. Questo approccio offre un elevato livello di sicurezza ed efficienza, consentendo una comunicazione sicura e affidabile tra il client e il server senza l'onere computazionale aggiuntivo associato alla crittografia asimmetrica.

Inoltre, QUIC implementa una serie di meccanismi di protezione aggiuntivi per garantire la sicurezza delle comunicazioni end-to-end. Questi includono l'utilizzo di firme digitali per garantire l'autenticità dei dati trasmessi e la protezione dei dati da eventuali manipolazioni durante il trasporto. Inoltre, QUIC supporta il rinnovamento periodico

delle chiavi crittografiche utilizzate durante la comunicazione, garantendo una sicurezza continua e resiliente nel tempo.[Aca20]

5.1.2 TLS 1.3

All'interno del contesto di QUIC, il supporto a TLS 1.3 rappresenta un altro importante pilastro per garantire la sicurezza delle comunicazioni. Transport Layer Security (TLS) è un protocollo crittografico ampiamente utilizzato per garantire la privacy e l'integrità delle informazioni trasmesse su Internet. La versione 1.3 di TLS rappresenta l'ultima evoluzione di questo protocollo e introduce una serie di miglioramenti significativi rispetto alle versioni precedenti.

Uno dei principali vantaggi di TLS 1.3 è rappresentato dalla sua maggiore efficienza e velocità. Rispetto alle versioni precedenti, TLS 1.3 riduce il numero di round-trip necessari per stabilire una connessione sicura, accelerando così il processo di handshake e riducendo la latenza complessiva della comunicazione. Questo è particolarmente importante in scenari in cui la velocità di risposta è critica, come nel caso del caricamento di pagine web o nell'avvio di sessioni di comunicazione in tempo reale.

Inoltre, TLS 1.3 offre una maggiore sicurezza rispetto alle versioni precedenti del protocollo. Introduce miglioramenti importanti nella gestione delle chiavi crittografiche e nell'algoritmo di handshake, rendendo più difficile per gli attaccanti intercettare o manipolare le comunicazioni protette da TLS. Inoltre, TLS 1.3 elimina alcune vulnerabilità presenti nelle versioni precedenti, come il padding dell'handshake e le modalità di cifratura obsolete, garantendo una protezione più robusta contro una vasta gamma di attacchi crittografici.

Un altro vantaggio di TLS 1.3 è rappresentato dalla sua maggiore resistenza agli attacchi di downgrade. Questo tipo di attacchi si basa sull'obbligare le comunicazioni a utilizzare versioni meno sicure del protocollo TLS, compromettendo così la sicurezza della connessione. TLS 1.3 implementa meccanismi avanzati per rilevare e prevenire tali attacchi, garantendo che le comunicazioni avvengano utilizzando sempre la versione più sicura del protocollo disponibile.

Inoltre, TLS 1.3 introduce miglioramenti significativi nella gestione della privacy degli utenti. Con questa versione del protocollo, viene aumentata la protezione della privacy durante il processo di handshake, riducendo al minimo le informazioni scambiate tra il client e il server durante la negoziazione dei parametri di sicurezza. Questo contribuisce a ridurre il rischio di esporre informazioni sensibili sugli utenti durante le comunicazioni online.[Res18]

5.1.3 Protezione dalla Corruzione dei Dati

Un'altro aspetto fondamentale della sicurezza nel protocollo QUIC è La protezione dalla corruzione dei dati, poichè assicura che i dati trasmessi tra il client e il server mantengano la loro integrità durante il trasporto su Internet. Questo aspetto è fondamentale per garantire che i dati ricevuti siano esattamente gli stessi dei dati inviati, senza subire modifiche indesiderate o danneggiamenti. Per comprendere appieno come QUIC protegge i dati dalla corruzione, è necessario esaminare alcuni dei meccanismi implementati all'interno del protocollo.

Una delle tecniche utilizzate da QUIC per proteggere i dati dalla corruzione è l'utilizzo di checksum e hash. Durante la trasmissione dei dati, ogni pacchetto QUIC include un checksum calcolato sui dati stessi, che viene utilizzato dal destinatario per verificare

l'integrità dei dati ricevuti. Se i dati sono stati corrotti durante il trasporto, il checksum non corrisponderà ai dati effettivi, segnalando un errore di integrità e permettendo al destinatario di rifiutare i dati corrotti. Questo meccanismo fornisce un primo livello di protezione contro la corruzione dei dati e garantisce che i dati ricevuti siano stati trasmessi correttamente.[Fas]

In aggiunta ai checksum, QUIC utilizza anche hash crittografici per proteggere i dati dalla corruzione. Prima di inviare i dati, il mittente calcola un hash crittografico dei dati stessi utilizzando algoritmi sicuri come SHA-256. Questo hash crittografico viene quindi incluso nei pacchetti QUIC e inviato insieme ai dati stessi. Una volta che i dati vengono ricevuti dal destinatario, questo calcola nuovamente l'hash crittografico dei dati ricevuti e lo confronta con l'hash ricevuto dal mittente. Se i due hash corrispondono, ciò indica che i dati sono stati trasmessi correttamente e non sono stati corrotti durante il trasporto. In caso contrario, il destinatario può rifiutare i dati corrotti e richiedere una ritrasmissione.[Has]

Questi meccanismi di protezione dalla corruzione dei dati sono cruciali per garantire l'integrità delle comunicazioni su QUIC e assicurare che i dati trasmessi mantengano la loro integrità durante il trasporto su Internet. Grazie all'utilizzo di checksum e hash crittografici, QUIC offre un elevato livello di sicurezza contro la corruzione dei dati, garantendo che le comunicazioni siano affidabili e prive di alterazioni indesiderate. Questo contribuisce a garantire un'esperienza utente sicura e affidabile per gli utenti di applicazioni Chromium che utilizzano il protocollo QUIC per le loro comunicazioni online.

5.1.4 Resistenza agli Attacchi

La resistenza agli attacchi è un aspetto della sicurezza nel protocollo QUIC che mira a proteggere le comunicazioni online da una vasta gamma di minacce e vulnerabilità. Per comprendere appieno come QUIC affronta gli attacchi e garantisce la sicurezza delle comunicazioni, è importante esaminare alcuni dei meccanismi implementati all'interno del protocollo.

Una delle caratteristiche chiave di QUIC che contribuisce alla sua resistenza agli attacchi è il suo modello di comunicazione multiplexed. QUIC consente la trasmissione di dati multipli su una singola connessione, consentendo di evitare problemi di blocco del testa di linea e aumentando l'efficienza complessiva della comunicazione. Questo modello multiplexed rende più difficile per un attaccante individuare e intercettare dati sensibili, riducendo il rischio di attacchi di tipo DoS (Denial of Service) e attacchi di tipo spoofing.

Inoltre, QUIC implementa meccanismi di autenticazione avanzati per garantire che le comunicazioni siano autentiche e provenienti da fonti attendibili. Utilizzando firme digitali e certificati crittografici, QUIC verifica l'autenticità delle comunicazioni e protegge da attacchi di tipo man-in-the-middle, dove un attaccante cerca di intercettare o manipolare i dati durante la trasmissione. Questi meccanismi di autenticazione garantiscono che le comunicazioni su QUIC siano sicure e affidabili, proteggendo gli utenti da potenziali minacce online.[Per21]

Inoltre, QUIC è progettato per essere resiliente agli attacchi di tipo DoS, che mirano a sovraccaricare una rete o un servizio online con un elevato volume di richieste dannose. Il protocollo implementa meccanismi di controllo della congestione e di gestione delle risorse di rete per mitigare gli effetti di tali attacchi e garantire che il servizio rimanga disponibile per gli utenti legittimi. Questi meccanismi aiutano a proteggere

la disponibilità e l'affidabilità delle comunicazioni su QUIC, garantendo un'esperienza utente coerente e priva di interruzioni.

5.1.5 Rinnovamento delle Chiavi

Il rinnovamento delle chiavi,un'altro dei tanti aspetti della sicurezza in QUIC, mira a garantire una protezione continua e resiliente delle comunicazioni online nel tempo. Questo meccanismo è progettato per mitigare i rischi associati alla compromissione delle chiavi crittografiche e garantire che le comunicazioni rimangano sicure anche in presenza di potenziali vulnerabilità nel sistema.

QUIC implementa il rinnovamento periodico delle chiavi crittografiche utilizzate durante le comunicazioni tra il client e il server. Questo processo prevede la generazione e l'aggiornamento regolare delle chiavi crittografiche utilizzate per cifrare e decifrare i dati trasmessi su Internet. Il rinnovamento delle chiavi viene eseguito in modo sicuro e trasparente, senza interrompere le comunicazioni in corso o compromettere la sicurezza delle connessioni.

Ciò significa che, anche se una chiave crittografica viene compromessa o compromessa nel tempo, il sistema può sostituire rapidamente la chiave compromessa con una nuova chiave, garantendo che le comunicazioni rimangano protette da potenziali minacce e attacchi. Questo meccanismo di rinnovamento delle chiavi contribuisce in modo significativo alla sicurezza delle comunicazioni su QUIC, garantendo che le informazioni trasmesse rimangano confidenziali e protette nel tempo.

Inoltre, il rinnovamento regolare delle chiavi crittografiche aiuta a prevenire l'accumulo di dati crittografici che potrebbero diventare vulnerabili a attacchi di crittoanalisi nel tempo. Aggiornando periodicamente le chiavi crittografiche utilizzate durante le comunicazioni, QUIC riduce il rischio di compromissione delle chiavi e garantisce una protezione continua e resiliente delle comunicazioni online.[MT21]

5.1.6 Conclusione

Per finire quindi, i principi di sicurezza di QUIC si basano su una combinazione di crittografia end-to-end, TLS 1.3, protezione dai dati corrotti e resistenza agli attacchi. Questi meccanismi garantiscono che le comunicazioni su Internet siano protette da intercettazioni, manipolazioni e altri tipi di minacce alla sicurezza. Grazie ai suoi elevati standard di sicurezza e alla sua resilienza agli attacchi, QUIC rappresenta una soluzione affidabile per le comunicazioni online, offrendo agli utenti una maggiore tranquillità nel trasferimento dei dati su Internet.

5.2 Meccanismi di sicurezza implementati in The Chromium Project

Il progetto Chromium è noto per la sua attenzione alla sicurezza e alla protezione degli utenti durante la navigazione web. Nel corso degli anni, il progetto ha implementato una serie di meccanismi di sicurezza avanzati per proteggere gli utenti da una vasta gamma di minacce online. Questi meccanismi includono misure preventive per impedire l'accesso non autorizzato ai dati degli utenti, protezione da attacchi informatici e difese contro vulnerabilità del software. Esamineremo alcuni dei principali meccanismi di sicurezza implementati nel progetto Chromium e il loro impatto sulla sicurezza online.

5.2.1 Sandbox

Il sandboxing rappresenta uno dei meccanismi di sicurezza più avanzati e cruciali implementati nel progetto Chromium. Questo approccio rivoluzionario è fondamentale per garantire un ambiente di navigazione web sicuro, proteggendo gli utenti da una vasta gamma di minacce informatiche e vulnerabilità del software. Vediamo più nel dettaglio come il sandboxing viene implementato e quali sono i suoi impatti sulla sicurezza degli utenti.

Il sandboxing in Chromium è basato su un modello di sicurezza a livelli multipli che limita l'accesso e i privilegi dei processi del browser. Ciò significa che ogni scheda, processo e componente aggiuntivo eseguito all'interno del browser è isolato in un ambiente separato, chiamato "sandbox". Questo sandbox impedisce ai processi dannosi di interagire con il sistema operativo o con altri processi del browser, limitando così il loro impatto e riducendo la possibilità di danneggiare il sistema.

Il sandboxing opera attraverso una combinazione di tecniche di isolamento e controllo degli accessi. I processi all'interno del sandbox sono eseguiti con privilegi limitati e non hanno accesso diretto alle risorse sensibili del sistema operativo, come i file di sistema o i driver del kernel. Inoltre, il sandboxing impedisce ai processi dannosi di comunicare con altri processi del browser o di accedere ai dati degli utenti, garantendo così la sicurezza e la privacy degli utenti durante la navigazione web.

Uno dei principali vantaggi del sandboxing è la sua capacità di limitare l'espansione degli attacchi dannosi. Anche se un'attività dannosa riesce ad infiltrarsi nel browser, il suo impatto sarà limitato dal sandbox e non potrà accedere a risorse sensibili o danneggiare il sistema operativo. Questo riduce di tanto il rischio di compromissione del sistema e protegge gli utenti da exploit dannosi e malware.

Inoltre, il sandboxing rende più difficile per gli attaccanti sfruttare le vulnerabilità del browser per eseguire codice dannoso sul sistema degli utenti. Anche se un'attività dannosa riesce a sfruttare una vulnerabilità nel browser, il sandbox impedisce al codice dannoso di diffondersi e di danneggiare ulteriormente il sistema. Questo fornisce una barriera efficace contro gli attacchi informatici e protegge gli utenti da potenziali minacce online.[KD]

5.2.2 Politiche di Sicurezza Same-Origin

Le politiche di sicurezza same-origin rappresentano un altro elemento fondamentale per la sicurezza nel progetto Chromium. Queste politiche sono progettate per proteggere gli utenti dalle vulnerabilità legate alla condivisione di risorse tra origini diverse durante la navigazione web. Origini diverse si riferiscono a diversi siti web o domini, e le politiche same-origin limitano l'accesso ai dati tra le pagine web provenienti da origini diverse. Vediamo più nel dettaglio come queste politiche sono implementate e quali sono i loro impatti sulla sicurezza degli utenti.

Quando un browser carica una pagina web, applica le politiche di sicurezza same-origin per determinare se lo script all'interno di una pagina ha il permesso di accedere ai dati di un'altra pagina. Se due pagine condividono lo stesso origine (ovvero lo stesso protocollo, dominio e porta) allora lo script di una pagina può accedere ai dati dell'altra pagina senza restrizioni. Però, se due pagine hanno origini diverse, lo script di una pagina non può accedere direttamente ai dati dell'altra pagina a meno che non ci sia una politica esplicita che lo consenta.[Sam]

Le politiche di sicurezza same-origin aiutano a prevenire attacchi come l'iniezione di script dannosi e l'accesso non autorizzato ai dati degli utenti. Per esempio, un attacco cross-site scripting (XSS) si verifica quando uno script dannoso viene eseguito su una pagina web e riesce ad accedere ai dati sensibili dell'utente su un'altra pagina web a cui l'utente ha accesso. Le politiche same-origin impediscono a uno script di una pagina di accedere ai dati di un'altra pagina a meno che le due pagine non condividano lo stesso origine, diminuendo così il rischio di attacchi XSS e proteggendo la privacy e la sicurezza degli utenti.[Dem19]

Le politiche di sicurezza same-origin aiutano a proteggere gli utenti da altri tipi di attacchi come l'ingegneria sociale e l'accesso non autorizzato ai dati degli utenti. Limitando l'accesso ai dati tra origini diverse, le politiche same-origin riducono il rischio che informazioni sensibili possano essere compromesse o sottratte da terze parti non autorizzate. Questo contribuisce a garantire che le comunicazioni online siano protette e che gli utenti possano navigare in modo sicuro e privo di preoccupazioni su Chromium.

5.2.3 HTTPS e Certificati SSL/TLS

La promozione dell'utilizzo di HTTPS e dei certificati SSL/TLS è un altro dei principali meccanismi di sicurezza implementati nel progetto Chromium. HTTPS, acronimo di "HyperText Transfer Protocol Secure", è una versione crittografata e sicura del protocollo HTTP utilizzato per la trasmissione di dati su Internet. I certificati SSL/TLS sono utilizzati per garantire l'autenticità e la crittografia delle comunicazioni tra il browser e il server web, proteggendo così la privacy e la sicurezza degli utenti durante la navigazione web.[ION20]

Quando un utente accede a un sito web tramite HTTPS, il browser e il server stabiliscono una connessione sicura utilizzando il protocollo SSL/TLS. Questo processo implica lo scambio di chiavi crittografiche tra il browser e il server per cifrare e decifrare i dati trasmessi durante la sessione di navigazione. I certificati SSL/TLS vengono utilizzati per garantire l'autenticità del server e la sicurezza della connessione, fornendo una prova che il sito web è affidabile e autentico.

L'utilizzo di HTTPS e dei certificati SSL/TLS offre diversi vantaggi in termini di sicurezza per gli utenti di Chromium. Innanzitutto, crittografando le comunicazioni tra il browser e il server, HTTPS protegge gli utenti da intercettazioni e intercettazioni da parte di terze parti, garantendo che i dati trasmessi siano al sicuro e protetti. Questo è particolarmente importante quando si trasmettono informazioni sensibili come password, informazioni di pagamento e dati personali su Internet.[Don13]

Inoltre, l'utilizzo di HTTPS e dei certificati SSL/TLS contribuisce alla protezione contro gli attacchi di tipo man-in-the-middle, dove un attaccante cerca di intercettare o manipolare le comunicazioni tra il browser e il server. Grazie alla crittografia delle comunicazioni, HTTPS rende più difficile per gli attaccanti interferire con la trasmissione dei dati e protegge gli utenti da potenziali minacce alla sicurezza online.

Per questi motivi l'utilizzo di HTTPS e dei certificati SSL/TLS migliora anche la fiducia degli utenti nella sicurezza del sito web e della piattaforma di navigazione. I browser moderni, tra cui Chromium, mostrano un'icona di sicurezza accanto all'URL del sito web quando viene utilizzato HTTPS, fornendo agli utenti una conferma visiva che il sito è protetto e affidabile. Questo incoraggia gli utenti a navigare in modo sicuro e a fare affidamento sulle piattaforme che utilizzano protocolli di comunicazione sicuri.

5.2.4 Auto-Update

Il sistema di auto-update implementato nel progetto Chromium è un meccanismo di sicurezza proattiva che garantisce agli utenti l'accesso alle più recenti patch di sicurezza e agli aggiornamenti del software in modo tempestivo e automatizzato. Questo sistema è progettato per garantire che il browser rimanga sempre aggiornato e protetto dalle ultime minacce di sicurezza, fornendo agli utenti una protezione continua e affidabile durante la navigazione web.

Il processo di auto-update in Chromium è gestito in modo trasparente e automatico, senza richiedere alcuna azione da parte degli utenti. Quando vengono rilasciati nuovi aggiornamenti o patch di sicurezza, il browser verifica periodicamente la disponibilità di nuove versioni e le scarica automaticamente in background. Una volta completato il download, il browser applica automaticamente gli aggiornamenti e notifica agli utenti che è disponibile una nuova versione del software.

La tempestività degli aggiornamenti è fondamentale per garantire la sicurezza degli utenti durante la navigazione web. Le patch di sicurezza vengono rilasciate regolarmente per risolvere vulnerabilità e bug di sicurezza nel software, e il sistema di auto-update assicura che gli utenti ricevano queste patch immediatamente dopo il loro rilascio. Ciò significa che gli utenti sono protetti dalle ultime minacce di sicurezza e che il loro browser è sempre allineato con le migliori pratiche di sicurezza online.

Inoltre, il sistema di auto-update contribuisce a semplificare la gestione del software per gli utenti, eliminando la necessità di monitorare manualmente la disponibilità di nuovi aggiornamenti e di eseguire il processo di aggiornamento manualmente. Questo riduce il rischio che gli utenti rimangano esposti a vulnerabilità di sicurezza a causa di software obsoleto e garantisce che il browser sia sempre aggiornato e protetto.

Il sistema di auto-update in Chromium offre una maggiore affidabilità e stabilità del software nel tempo. Mantenendo il browser sempre aggiornato con le ultime correzioni di bug e miglioramenti delle prestazioni, il sistema di auto-update contribuisce a garantire un'esperienza utente fluida e priva di problemi durante la navigazione web. Gli utenti possono quindi navigare in modo sicuro e affidabile su Chromium, senza preoccuparsi di problemi di sicurezza o prestazioni del software.

5.2.5 Protezione Antiphishing e Antimalware

La protezione antiphishing e antimalware serve per proteggere gli utenti da siti web dannosi e contenuti maligni durante la navigazione web. Questo sistema di protezione si basa su una serie di tecniche e strumenti proattivi per rilevare e prevenire potenziali minacce online, fornendo agli utenti una navigazione sicura e priva di rischi.

Uno dei principali strumenti utilizzati per la protezione antiphishing e antimalware in Chromium è la lista di URL dannosi, che viene costantemente aggiornata e mantenuta dal team di sviluppo del browser. Questa lista contiene gli URL noti di siti web dannosi, phishing e malware, e il browser verifica automaticamente ogni URL visitato dall'utente contro questa lista per identificare e avvertire gli utenti in caso di potenziali minacce.

Inoltre, Chromium integra funzionalità di rilevamento e scansione antivirus per identificare e bloccare file dannosi e malware durante il download o l'apertura su una pagina web. Questo sistema di protezione antimalware utilizza motori di scansione avanzati per analizzare i file in tempo reale e rilevare eventuali segni di malware o contenuti dannosi, proteggendo così gli utenti da potenziali infezioni e danni al sistema.

Oltre alla lista di URL dannosi e alle funzionalità di scansione antivirus, Chromium utilizza anche strumenti avanzati di analisi del comportamento per identificare e bloccare siti web sospetti o comportamenti dannosi durante la navigazione web. Questi strumenti monitorano costantemente il comportamento del browser e delle pagine web visitate dagli utenti per rilevare eventuali attività sospette o anomale e avvertire gli utenti in tempo reale.

Chromium collabora attivamente con motori di ricerca e fornitori di servizi di sicurezza per identificare e bloccare siti web e contenuti dannosi prima che possano danneggiare gli utenti. Questa collaborazione permette di mantenere costantemente aggiornata la lista di URL dannosi e di reagire prontamente alle nuove minacce online, fornendo agli utenti una protezione avanzata e affidabile durante la navigazione web.

5.2.6 Rete di Segnalazione delle Vulnerabilità (Vulnerability Reporting Network)

La rete di segnalazione delle vulnerabilità (Vulnerability Reporting Network) svolge un ruolo fondamentale nella sicurezza del browser e nella protezione degli utenti da potenziali minacce online. Questa rete fornisce una piattaforma centralizzata e sicura per la segnalazione e la gestione delle vulnerabilità del software, consentendo agli utenti e ai ricercatori della sicurezza di segnalare eventuali problemi di sicurezza scoperti durante l'utilizzo del browser.

La rete di segnalazione delle vulnerabilità permette agli utenti e ai ricercatori della sicurezza di segnalare eventuali vulnerabilità o bug di sicurezza scoperti nel software Chromium al team di sviluppo del browser. Questo processo di segnalazione avviene attraverso canali dedicati e protetti, che garantiscono la riservatezza delle informazioni sensibili e la protezione degli utenti che segnalano le vulnerabilità.

Una volta ricevuta una segnalazione di vulnerabilità, il team di sviluppo del browser valuta immediatamente il problema e avvia il processo di risoluzione. Questo può comprendere la ricerca della causa del problema, lo sviluppo di una patch di sicurezza e la distribuzione di un aggiornamento del software per risolvere la vulnerabilità. La rete di segnalazione delle vulnerabilità consente al team di sviluppo di rispondere prontamente alle minacce di sicurezza e di proteggere gli utenti da potenziali exploit e attacchi informatici.

La rete di segnalazione delle vulnerabilità può anche includere funzionalità di monitoraggio e analisi del comportamento del software per rilevare e prevenire potenziali minacce di sicurezza. Questi strumenti avanzati consentono al team di sviluppo di identificare e rispondere rapidamente alle nuove minacce di sicurezza, proteggendo gli utenti da potenziali exploit e attacchi informatici. Questa può includere anche programmi di ricompense per la segnalazione delle vulnerabilità, che offrono incentivi finanziari per coloro che scoprono e segnalano vulnerabilità nel software Chromium. Questi programmi motivano i ricercatori della sicurezza a contribuire attivamente alla sicurezza del browser e a collaborare con il team di sviluppo per identificare e risolvere potenziali minacce di sicurezza.

5.2.7 Conclusione

In conclusione, il progetto Chromium implementa una serie di meccanismi di sicurezza avanzati per proteggere gli utenti durante la navigazione web. Dal sandboxing e dalle politiche di sicurezza same-origin, all'adozione di HTTPS e certificati SSL/TLS, al

sistema di auto-update e alla protezione antiphishing e antimalware, Chromium offre una piattaforma sicura e affidabile per la navigazione web. La rete di segnalazione delle vulnerabilità garantisce che il progetto rimanga sempre all'avanguardia nella lotta contro le minacce di sicurezza online, proteggendo gli utenti da potenziali vulnerabilità e attacchi informatici.

5.3 Impatto delle caratteristiche di sicurezza di QUIC nell'ecosistema Chromium

Quando esaminiamo l'impatto delle caratteristiche di sicurezza di QUIC nell'ecosistema Chromium, è importante considerare anche aspetti meno evidenti ma altrettanto significativi. Una di queste caratteristiche è la capacità di QUIC di ridurre l'esposizione agli attacchi di fingerprinting. Il fingerprinting è una tecnica utilizzata dagli aggressori per identificare e tracciare gli utenti online basandosi sulle loro caratteristiche uniche di navigazione e dispositivo. Questa pratica sfrutta varie informazioni raccolte dai browser web, come ad esempio l'User-Agent, i cookie, le informazioni sul dispositivo e altre caratteristiche tecniche, per creare un "fingerprint" unico per ciascun utente. Questo fingerprint può essere utilizzato per identificare e tracciare gli utenti attraverso diverse sessioni di navigazione e siti web, consentendo agli aggressori di creare profili dettagliati sugli utenti e di raccogliere informazioni sensibili su di loro. Grazie alla crittografia integrata e alla natura multiplexing delle connessioni QUIC, è più difficile per gli aggressori identificare e tracciare gli utenti basandosi sulle loro attività di navigazione, contribuendo così a preservare la privacy degli utenti su Internet.[WIR22]

Inoltre, QUIC offre vantaggi significativi anche per quanto riguarda la protezione contro attacchi di tipo timing side-channel. Il timing side-channel è una tecnica utilizzata dagli aggressori per inferire informazioni sensibili sulle attività degli utenti sfruttando le differenze di tempo nelle risposte del server. In altre parole, gli aggressori monitorano attentamente il tempo necessario per completare determinate operazioni o ricevere risposte da un server durante una comunicazione web e utilizzano queste informazioni per ricavare dati sensibili come password, chiavi di crittografia o altre informazioni riservate. Grazie alla sua natura di trasporto multiplexato, QUIC può ridurre l'accuratezza di questi attacchi, complicando la raccolta di informazioni sensibili sugli utenti e migliorando la loro sicurezza online.[Wri]

Un altro aspetto da considerare è la capacità di QUIC di facilitare l'adozione di politiche di sicurezza più avanzate come Content Security Policy (CSP) e Subresource Integrity (SRI).

Content Security Policy (CSP) e Subresource Integrity (SRI) sono due meccanismi di sicurezza fondamentali utilizzati per proteggere le applicazioni web da vari tipi di attacchi, tra cui l'iniezione di script dannosi e il caricamento di risorse non autorizzate. Entrambi sono stati integrati nell'ecosistema Chromium insieme all'implementazione di QUIC, contribuendo a rafforzare ulteriormente la sicurezza delle applicazioni web.

Content Security Policy (CSP) è un insieme di direttive che consentono agli sviluppatori di specificare quali risorse esterne (come script JavaScript, fogli di stile CSS, font, immagini, etc.) possono essere caricati e da dove. Ciò significa che gli sviluppatori possono limitare l'esecuzione di codice JavaScript non fidato, riducendo così il rischio di attacchi di tipo XSS (Cross-Site Scripting) e l'iniezione di script dannosi nelle loro applicazioni. Con CSP, è possibile definire una serie di regole che indicano al brow-

ser quali domini sono considerati attendibili per il caricamento di risorse, limitando le vulnerabilità legate all'esecuzione di codice non fidato.[Gui]

Subresource Integrity (SRI), d'altra parte, è una tecnica che consente agli sviluppatori di garantire l'integrità delle risorse esterne caricate nelle loro pagine web. Questo viene fatto aggiungendo un hash crittografico alla definizione delle risorse esterne (come script JavaScript, fogli di stile CSS, immagini, etc.) nel markup HTML. Quando il browser riceve la pagina web, verifica che l'hash delle risorse corrisponda a quello specificato nella definizione. Se l'hash non corrisponde, il browser rifiuta di caricare la risorsa, impedendo così il caricamento di risorse modificate o compromesse.[dev]

Queste politiche consentono agli sviluppatori di controllare e mitigare il rischio di iniezione di script dannosi o il caricamento di risorse non autorizzate all'interno delle loro applicazioni web. Grazie alla sua architettura e alle sue caratteristiche avanzate, QUIC può semplificare l'implementazione e l'esecuzione di queste politiche, migliorando la sicurezza complessiva delle applicazioni web su Chromium.

Infine, vale la pena considerare l'impatto di QUIC sulla protezione degli utenti contro attacchi di tipo spoofing e man-in-the-middle. Lo spoofing si verifica quando un attaccante imita un'altra entità, come un sito web o un utente legittimo, al fine di ottenere informazioni sensibili o condurre azioni dannose. Il man-in-the-middle, invece, avviene quando un aggressore si interpone tra due parti che comunicano, intercettando e possibilmente alterando le comunicazioni tra di loro. Grazie alla sua natura di trasporto multiplexato e alla gestione intelligente delle connessioni, QUIC può ridurre significativamente il rischio di intercettazione e manipolazione delle comunicazioni da parte di aggressori malevoli, proteggendo così gli utenti da attacchi di phishing, spoofing e altri tipi di frodi online.

Per concludere, l'impatto delle caratteristiche di sicurezza di QUIC nell'ecosistema Chromium va oltre la semplice crittografia e la protezione delle connessioni Internet. QUIC offre una serie di vantaggi aggiuntivi che contribuiscono a preservare la privacy degli utenti, migliorare la sicurezza delle applicazioni web e proteggere gli utenti da una grande varietà di minacce online. Questi benefici rendono QUIC non solo una scelta ottimale per migliorare le prestazioni delle connessioni Internet, ma anche un importante strumento per garantire una navigazione web sicura e priva di rischi su Chromium.

6. Conclusioni

6.1 Riassunto delle principali scoperte

L'analisi dettagliata dell'impatto di QUIC nell'ecosistema Chromium ha evidenziato una serie di vantaggi importanti che influenzano positivamente sia la sicurezza che le prestazioni della navigazione web. Uno degli aspetti più distintivi e fondamentali di QUIC è la sua capacità di fornire una crittografia integrata, la quale comprende un robusto meccanismo di protezione per le comunicazioni tra il browser e il server. Questa crittografia avanzata garantisce che le informazioni scambiate durante una sessione di navigazione siano protette da potenziali intercettazioni o manipolazioni malevole da parte di terze parti.

La presenza di una crittografia integrata aggiunge uno strato in più di sicurezza fondamentale per garantire che i dati sensibili degli utenti, come le informazioni personali, dati finanziari o altro, rimangano al sicuro durante la loro attività online. Questa sicurezza è fondamentale in un mondo digitale sempre più complesso e pericoloso, in cui gli attacchi informatici e le violazioni della privacy sono sempre più diffusi.

In aggiunta alla crittografia integrata, la natura multiplexata delle connessioni QUIC offre ulteriori vantaggi in termini di sicurezza e privacy degli utenti. Questo metodo di trasporto consente al browser di inviare e ricevere dati multipli attraverso una singola connessione, creando un ambiente web più sicuro e protetto per gli utenti di Chromium. La multiplexazione dei dati non solo migliora l'efficienza delle comunicazioni, ma rende anche più difficile per gli aggressori identificare e tracciare gli utenti online. Poiché i dati vengono trasportati in pacchetti multipli all'interno di una singola connessione, il traffico risulta meno suscettibile a tecniche di analisi e di tracciamento, riducendo il rischio di profilazione indesiderata e preservando così la privacy degli utenti su Internet. Questa nuova forma di comunicazione online rappresenta un'importante difesa contro attacchi informatici e tentativi di violazione della privacy su Internet, contribuendo a creare un ambiente online più sicuro e protetto per tutti gli utenti di Chromium.

Inoltre, QUIC rivoluziona il modo in cui gli sviluppatori possono implementare politiche di sicurezza avanzate, come Content Security Policy (CSP) e Subresource Integrity (SRI), offrendo loro strumenti potenti per proteggere le loro applicazioni web da una vasta gamma di attacchi informatici e vulnerabilità di sicurezza.

Content Security Policy (CSP) è un meccanismo di sicurezza che permette agli sviluppatori di definire regole precise sulle fonti da cui possono essere caricate risorse, come script JavaScript, immagini o stili CSS. Queste regole consentono agli sviluppatori di mitigare il rischio di attacchi di tipo XSS (Cross-Site Scripting) e l'iniezione di script dannosi, limitando il caricamento di risorse da origini non attendibili o non autorizzate.

Subresource Integrity (SRI), d'altra parte, è un'altra tecnica di sicurezza che consente agli sviluppatori di verificare l'integrità delle risorse esterne caricate nelle loro

pagine web. Questo viene fatto aggiungendo un hash crittografico alla definizione delle risorse esterne nel markup HTML. Quando il browser riceve la pagina web, verifica che l'hash delle risorse corrisponda a quello specificato nella definizione. Se l'hash non corrisponde, il browser rifiuta di caricare la risorsa, impedendo così il caricamento di risorse modificate o compromesse.

L'integrazione di queste politiche di sicurezza avanzate con QUIC offre agli sviluppatori una protezione completa contro una vasta gamma di attacchi informatici e vulnerabilità di sicurezza. La combinazione di crittografia integrata, natura multiplexata delle connessioni e supporto per politiche di sicurezza avanzate rende le applicazioni web più sicure e robuste, offrendo agli utenti una maggiore protezione e tranquillità durante la navigazione online.

6.2 Riflessioni sull'importanza di QUIC nel contesto di Chromium

L'implementazione di QUIC nell'ecosistema di Chromium ha suscitato riflessioni fondamentali sull'importanza di questa tecnologia emergente nel contesto della navigazione web moderna. QUIC non è semplicemente un nuovo protocollo di trasporto, ma rappresenta un importante passo avanti verso una navigazione web più sicura, efficiente e all'avanguardia.

L'integrazione di QUIC ha notevolmente potenziato la sicurezza della navigazione web su Chromium. Grazie alla sua crittografia integrata e alla capacità di resistere agli attacchi di tipo timing side-channel, QUIC ha contribuito a proteggere i dati sensibili degli utenti da intercettazioni e manipolazioni malevole. Questo ha posto una nuova pietra miliare nella protezione della privacy online e nella mitigazione dei rischi legati alla sicurezza informatica.

La crittografia integrata offerta da QUIC rappresenta uno strumento fondamentale per proteggere le comunicazioni tra il browser e il server da eventuali minacce esterne. Con QUIC, le informazioni scambiate durante una sessione di navigazione sono crittografate in modo robusto, rendendo estremamente difficile per gli aggressori intercettare o manipolare i dati trasmessi. Questo livello aggiuntivo di sicurezza è cruciale per garantire che i dati sensibili degli utenti rimangano al sicuro durante la navigazione online.

Inoltre, la resistenza di QUIC agli attacchi di tipo timing side-channel rappresenta un'importante difesa contro forme avanzate di manipolazione dei dati. Questi attacchi sfruttano le variazioni di tempo nelle risposte del server per estrarre informazioni sensibili o identificare vulnerabilità nel sistema. Grazie alla sua architettura progettata per mitigare questo tipo di attacchi, QUIC offre una maggiore protezione contro minacce sofisticate che potrebbero compromettere la sicurezza delle comunicazioni online.

Come anticipato anche nel sottocapitolo precedente, QUIC ha introdotto miglioramenti significativi nelle prestazioni della navigazione web su Chromium. La natura multiplexata delle sue connessioni infatti ha ridotto i tempi di caricamento delle pagine e ottimizzato l'utilizzo della larghezza di banda, offrendo agli utenti un'esperienza di navigazione più fluida e reattiva. Inoltre, l'ottimizzazione delle prestazioni su dispositivi mobili ha contribuito a prolungare la durata della batteria e migliorare l'efficienza energetica dei dispositivi mobili durante la navigazione web.

Un altro punto cruciale riguarda la flessibilità e l'adattabilità di QUIC a diverse architetture di rete e tecnologie emergenti. Questa caratteristica essenziale di QUIC

consente al protocollo di integrarsi agevolmente con una vasta gamma di infrastrutture di rete, garantendo una connettività affidabile e uniforme per gli utenti di Chromium in tutto il mondo.

QUIC è stato progettato per funzionare efficacemente su reti di vario genere, comprese quelle caratterizzate da alta latenza, perdita di pacchetti o congestionamento. La sua capacità di adattarsi dinamicamente alle mutevoli condizioni di rete consente di garantire prestazioni ottimali in qualsiasi contesto, migliorando l'esperienza complessiva degli utenti durante la navigazione web.

Grazie alla sua flessibilità e adattabilità, QUIC si presenta come una soluzione ideale per affrontare le sfide sempre più complesse dell'ambiente di rete odierno e futuro. La sua capacità di integrarsi con successo in una vasta gamma di contesti di rete e tecnologie emergenti ne fa uno strumento prezioso per garantire una connettività affidabile e prestazioni ottimali per gli utenti di Chromium in tutto il mondo.

L'introduzione di QUIC ha stimolato l'innovazione nel panorama della navigazione web, aprendo nuove opportunità per gli sviluppatori e promuovendo lo sviluppo di applicazioni web più avanzate e interattive. Gli sviluppatori possono ora sfruttare le prestazioni ottimizzate offerte da QUIC per creare esperienze utente coinvolgenti e innovative, portando a una nuova generazione di applicazioni web che offrono agli utenti un'esperienza simile a quella delle applicazioni native.

In conclusione, QUIC rappresenta un elemento chiave nell'evoluzione di Chromium e nel miglioramento dell'esperienza complessiva degli utenti durante la navigazione web. Il suo impatto positivo sulla sicurezza, sulle prestazioni e sull'innovazione ha consolidato la sua posizione come uno dei pilastri fondamentali dell'ecosistema di Chromium, promettendo di continuare a guidare l'evoluzione della navigazione web verso nuovi orizzonti.

Bibliografia

[Aca20] Binance Academy. «Cos'è la Crittografia End-to-End (E2EE)?» In: *Binance Academy* (2020). URL: https://academy.binance.com/it/articles/what-is-end-to-end-encryption-e2ee.

[Ahm16] Arif Ahmed. Ejaz Ahmed. *A Survey on Mobile Edge Computing*. 2016. URL: https://www.researchgate.net/publication/285765997_A_Survey_on_Mobile_Edge_Computing.

[Bis22] Mike Bishop. «HTTP/3. RFC 9114». In: *IETF Datatracker* (2022). URL: https://datatracker.ietf.org/doc/html/rfc9114.

[Com13] Douglas E. Comer. *Internetworking With TCP/IP Vol I: Principles, Protocols, and Architecture*. 2013. URL: https://www.homeworkforyou.com/static_media/uploadedfiles/Douglas%20E.%20Comer%20-%20Internetworking%20with%20TCP_IP%20Volume%20One.%201-Addison-Wesley%20(2013).pdf.

[Cor] Coretech. «Il protocollo HTTP3 e Quic». In: *Coretech* (). URL: https://www.coretech.it/it/service/knowledge_base/Sicurezza/Sviluppo-Sicuro/Il-protocollo-HTTP3-e-Quic.php.

[Dem19] Oliviero Demicheli. «Cross-site Scripting: come funziona un attacco XSS e come proteggersi». In: *cybersecurity360.it* (2019). URL: https://www.cybersecurity360.it/nuove-minacce/cross-site-scripting-come-funziona-un-attacco-xss-e-come-proteggersi/.

[dev] developer.mozilla.org. «Subresource Integrity». In: *developer.mozilla.org* (). URL: https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity.

[Difa] In: (). URL: https://technos.wordpress.com/2010/06/26/le-differenze-tra-google-chrome-e-chromium/.

[Difb] In: (). URL: https://technos.wordpress.com/2010/06/26/le-differenze-tra-google-chrome-e-chromium/.

[Don13] Brian Donohue. «Digital Certificates and 'HTTPS'». In: *Kaspersky daily* (2013). URL: https://www.kaspersky.com/blog/digital-certificates-https/1797/.

[Fas] FasterCapital. «Esplorare l importanza del checksum nell integrita dei dati». In: *FasterCapital* (). URL: https://fastercapital.com/it/contenuto/Esplorare-l-importanza-del-checksum-nell-integrita-dei-dati.html#Comprensione-delle-basi-del-checksum.

[FC21] Marco Giordani Kostantinos Antonakoglou Toktam Mahmoodi Andrea Zanella Federico Chiariotti Anay Ajit Deshpande. *QUIC-EST: a QUIC-Enabled Scheduling and Transmission Scheme to Maximize VoI with Correlated Data Flows*. 2021. URL: https://www.dei.unipd.it/~zanella/PAPER/CR_2021/commag-quic-scheduling-final.pdf.

[Fot] In: (). URL: https://learn.microsoft.com/it-it/azure/rtos/netx-duo/netx-secure-tls/chapter3.

[Ghe19] Alessandro Ghedini. «Even faster connection establishment with QUIC 0-RTT resumption». In: *The Cloudflare Blog* (2019). URL: https://blog.cloudflare.com/even-faster-connection-establishment-with-quic-0-rtt-resumption.

[Goo08] Google. «Chromium». In: *Wikipedia* (2008). URL: https://en.wikipedia.org/wiki/Chromium_(web_browser).

[Gui] Content Security Policy (CSP) Quick Reference Guide. «Content Security Policy Reference». In: *Content Security Policy (CSP) Quick Reference Guide* (). URL: https://content-security-policy.com/#:~:text=Content%2DSecurity%2DPolicy%20is%20the,they%20can%20be%20loaded%20from..

[Has] «Secure Hash Algorithm». In: *Wikipedia* (). URL: https://it.wikipedia.org/wiki/Secure_Hash_Algorithm.

[Htt] In: (). URL: https://www.debugbear.com/blog/http3-quic-protocol-guide.

[Imma] In: (). URL: https://en.wikipedia.org/wiki/Head-of-line_blocking.

[Immb] In: (). URL: https://blog.saverioriotto.it/.

[Immc] In: (). URL: https://trasformazionedigitale.bit4id.com/cultura-digitale/crittografia-end-to-end-come-protegge/.

[ION20] IONOS. «HTTPS: cosa significa e perché è così importante». In: *IONOS* (2020). URL: https://www.ionos.it/digitalguide/hosting/tecniche-hosting/cose-https/.

[JI21a] Ian Swett Jana Iyengar. «QUIC Loss Detection and Congestion Control. RFC 9002». In: *IETF Datatracker* (2021). URL: https://datatracker.ietf.org/doc/html/rfc9002.

[JI21b] Martin Thomson Jana Iyengar. «QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000». In: *IETF Datatracker* (2021). URL: https://datatracker.ietf.org/doc/rfc9000/.

[KD] Kayla Nussbaum Kelly Trainor Kayla Davis Shayde Nofziger. *A Case Study: Chromium Vulnerability History*. URL: https://www.se.rit.edu/~swen-331/projects/case-study/ChromiumCaseStudy.pdf.

[MG21] Mohammad Salahuddin R. Boutaba Milad Ghaznavi Elaheh Jalalpour. *1Content Delivery Network Security: A Survey*. 2021. URL: https://www.researchgate.net/publication/352847355_Content_Delivery_Network_Security_A_Survey.

[MP20] F. Michel F. Rochet O. Bonaventure M. Piraux Q. De Coninck. ≪QUIC Plugins≫. In: *IETF Datatracker* (2020). URL: https://www.ietf.org/archive/id/draft-piraux-quic-plugins-00.html.

[MT21] Sean Turner Martin Thomson. ≪Using TLS to Secure QUIC, RFC 9001≫. In: *IETF Datatracker* (2021). URL: https://datatracker.ietf.org/doc/html/rfc9001.

[Per21] Giorgio Perego. ≪L'attacco Man in the Middle: cos'è e come funziona≫. In: *Insic.it* (2021). URL: https://www.insic.it/privacy-e-sicurezza/information-security/lattacco-man-in-the-middle-cose-e-come-funziona/.

[Res18] Eric Rescorla. ≪The Transport Layer Security (TLS) Protocol Version 1.3 RFC 8446≫. In: *IETF Datatracker* (2018). URL: https://datatracker.ietf.org/doc/html/rfc8446.

[Sam] ≪Same origin policy≫. In: *Wikipedia* (). URL: https://it.wikipedia.org/wiki/Same_origin_policy#:~:text=La%20regola%20permette%20agli%20script,pagine%20provenienti%20da%20siti%20diversi..

[Ste] In: (). URL: https://github.com/chromium.

[Ult] In: (). URL: https://www.twingate.com/blog/tcp-vs-udp.

[WIR22] WIRED. ≪Che cos'è il fingerprinting e quanto dobbiamo preoccuparcene≫. In: *WIRED* (2022). URL: https://www.wired.it/article/fingerprinting-cosa-e-tracciamento/.

[Wri] Gavin Wright. ≪timing attack≫. In: *TechTarget* (). URL: https://www.techtarget.com/searchsecurity/definition/timing-attack#:~:text=A%20timing%20attack%20is%20a,attacks%20against%20some%20encryption%20methods..

Ringraziamenti

Ringrazio...