



IT-Sicherheit

9 QUIC-Protokoll http 1.3



Gerrit Kalkbrenner
Gerrit.Kalkbrenner@hwr-berlin.de

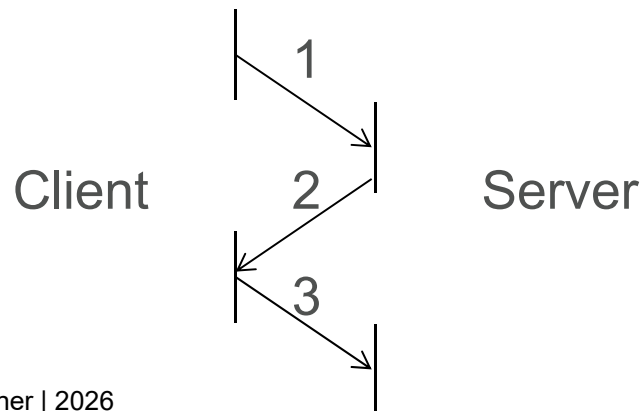
QUIC - ein neues Transport-Protokoll

- Im Internet bahnt sich eine umwälzende Änderung an, die zu schnelleren Übertragungen führen wird
- von Google angestoßen
- Ablösung von TCP
- Beschleunigter Aufbau von Web-Seiten
- QUIC = Quick UDP Internet Connection



Entwicklungen

- Rasante Geschwindigkeitssteigerung des Internet
- Selbst Privatanwender haben Gigabit-Anschlüsse
- TCP schöpft Geschwindigkeit nicht aus
- Üblich: 3 Wege-Handshake





Zugriff auf Web-Seiten

Aufbau einer Verbindung:

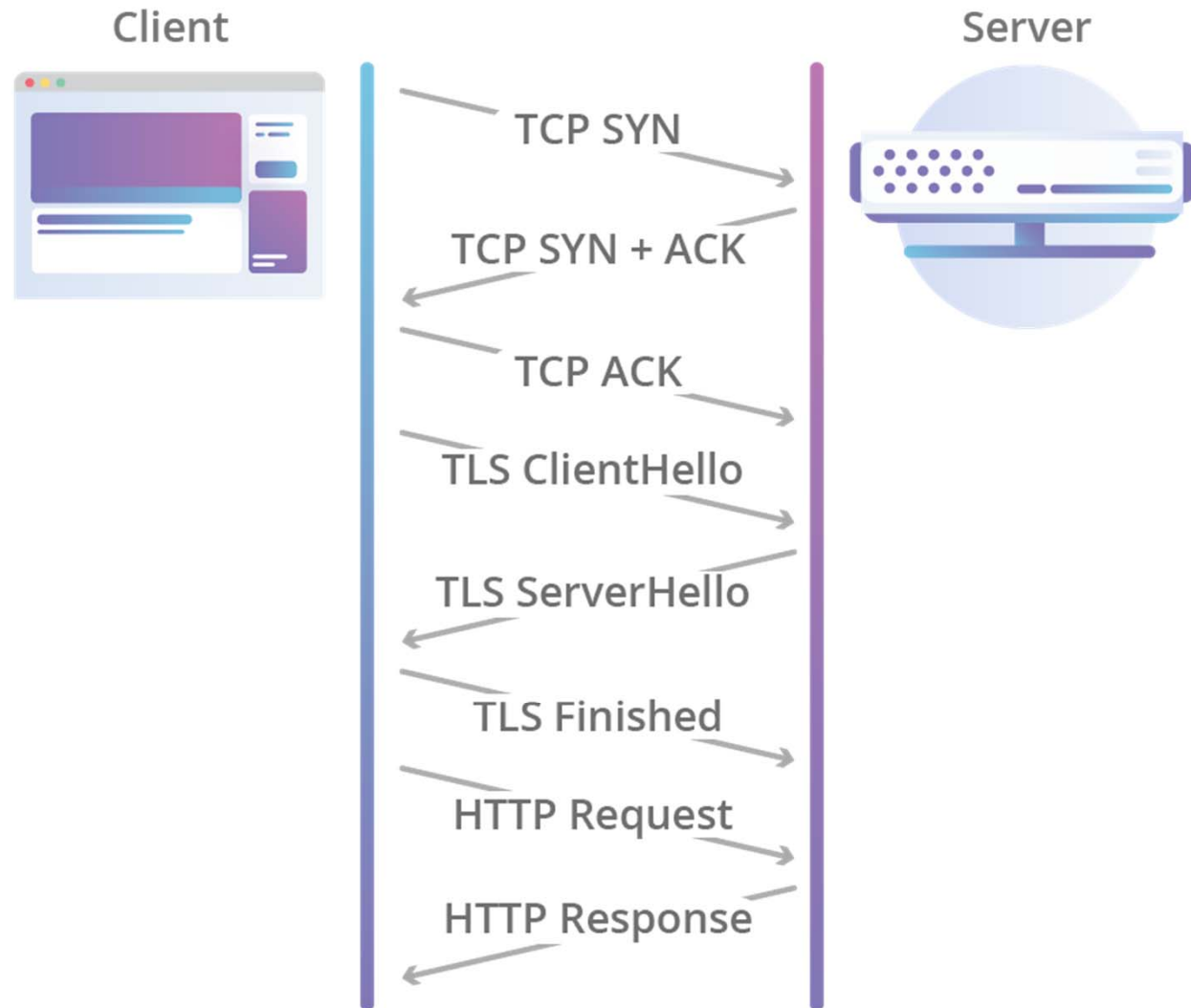
1. 3 Wege Handshake für TCP
 2. Handshake für TLS, Aushandeln der Sicherheit
 3. Handshake HTTP
- Klingt nach wenig, summiert sich aber für aus etlichen Teilen bestehenden Web-Seiten
 - Vorgehen so weit wie möglich verkürzen!

QUIC - Quick UDP Internet Connections

- 2012 bei Google begonnen
- Verschachtelung der Handshake-Wartezeiten
- Sehr Erfolgsversprechend, daher 2017 Übergabe an die IETF
- Neu dafür: HTTP/3, TLS 1.3
- Inzwischen die Hälfte des Verkehrs zwischen Google Servern und Chrome mit QUIC
- Facebook komplett, beta in Edge, Firefox, Safari

TCP+ TLS

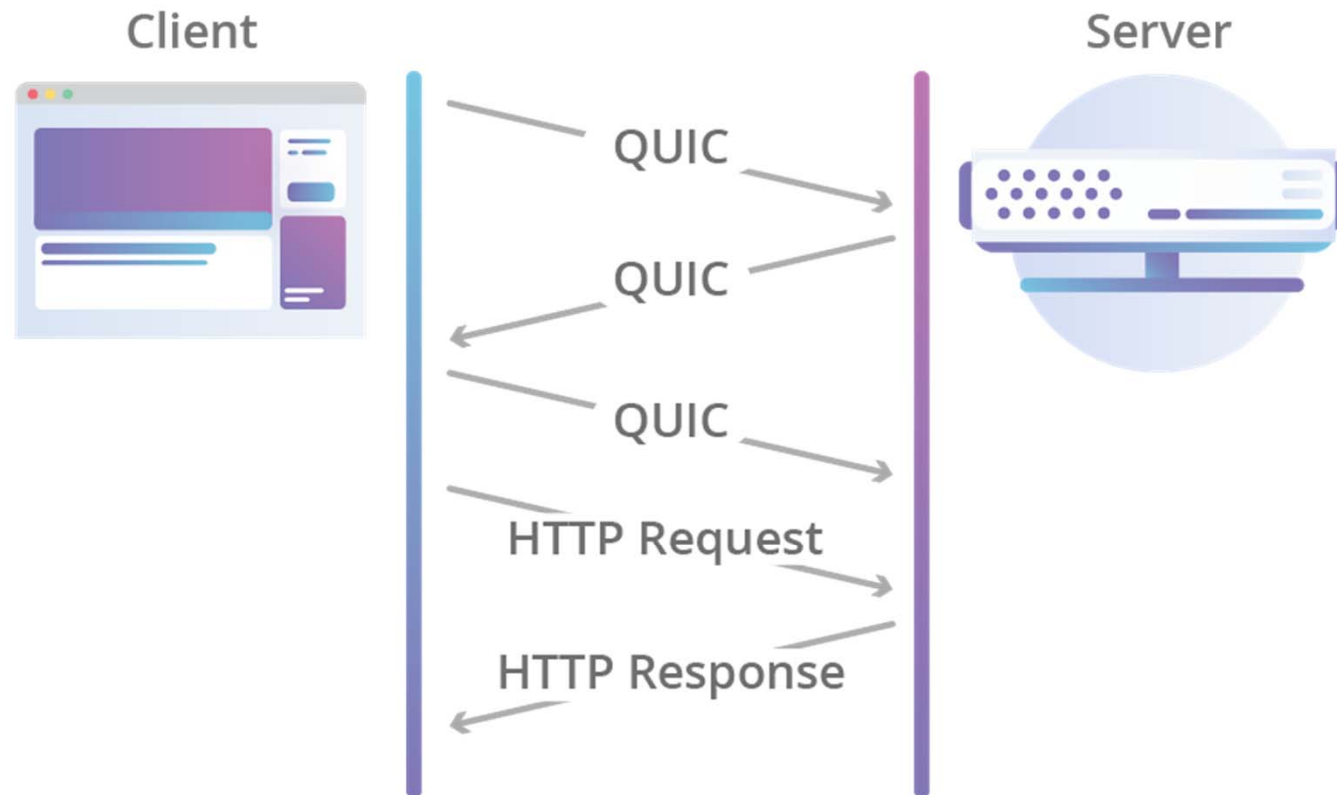
HTTP Request Over TCP + TLS



Quelle: Alessandro Ghedini

QUIC

HTTP Request Over QUIC





Potenzial

- Bei Round Trip von 200 mS
- HTTPS: oft bis zu 2 Sekunden für den Aufbau
- Komplexes Protokoll: 3 Schritte auf einem mal
- Was passiert, wenn ein Schritt scheitert?
- QUIC bietet ausschließlich Verschlüsselung
- Rechenzentren und NSA wollen gerne mithören