CERIAS
The Center for Education and Research in Information Assurance and Security

How Secure and Quick is QUIC? Provable Security and Performance Analyses

Robert Lychev, Samuel Jero, Alexandra Boldyreva, and Cristina Nita-Rotaru
Georgia Institute of Technology and Purdue University

To appear in IEEE Symposium on Security & Privacy 2015 (Oakland)

QUIC: Quick UDP Internet Connections

- Provides authenticated, encrypted byte-stream connections between hosts similar to TLS over TCP
- Zero round trip connection establishment on repeat connections for reduced latency
- Developed by Google and deployed in Chrome in 2013

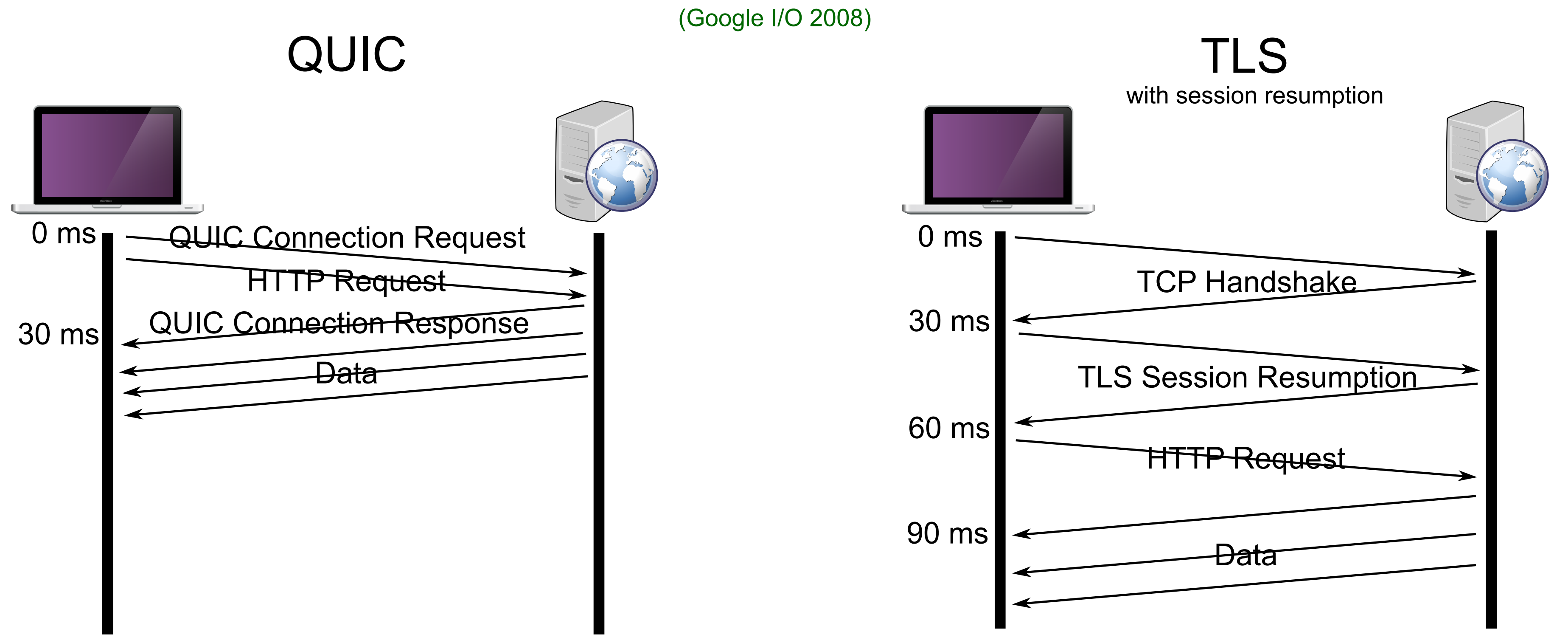
How Secure is QUIC actually?

- QUIC is about 3 years old
- SSL/TLS is 6 versions and 20 years old
- Existing security analyses of QUIC do not consider the protocol as actually specified or are formulated informally

Latency is Money

500ms of additional latency results in a 20% drop in Google searches

(Google I/O 2008)



Initial Latency: 30ms

Initial Latency: 90ms

Provable Security

A formal proof of a protocol under a specific security model specifying the security properties preserved, assumptions made, and the adversary's capabilities

Existing Models:

- ACCE (Authenticated and Confidential Channel Establishment)
- EMV
- Cannot be reused for QUIC due to multiple session keys, lack of TCP, and key exchange/ data exchange overlap

New Model

QACCE: Quick Authenticated and Confidential Channel Establishment

Designed for protocols with:

- Initial Key Agreement
- Initial Data Exchange
- Key Agreement
- Data Exchange

Considers:

- The security of the protocol under chosen plain-text attack
- The authenticity of delivered messages
- Forward secrecy after a period of time
- Attackers who impersonate honest servers
- IP Spoofing

QUIC is QACCE if the signature scheme is suf-cma and the encryption scheme is is ind-cpa- and auth-secure and the Strong Computational Diffie-Hellman problem is hard, in the random oracle model

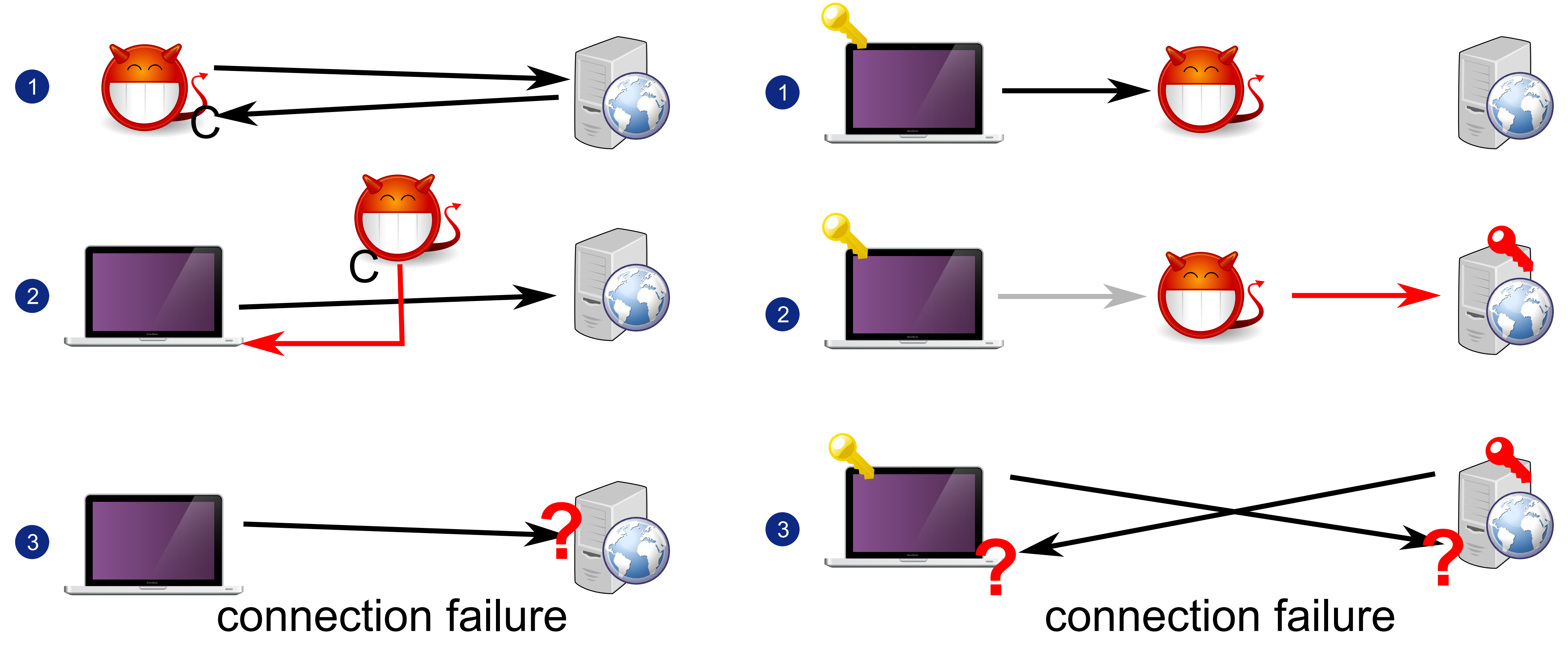
Performance and Malice

We identified several attacks on QUIC which impact performance

- Client Denial-of-Service
  - Replay Attacks
  - Manipulation Attacks
  - Byte-stream Attacks
- Server Denial-of-Service
  - Replay Attacks
- Attacks do not compromise security, only performance
- Attacks on TLS's performance exist, but TLS makes no performance claims

Replay Attack

Manipulation Attack



Despite these attacks, QUIC provides security guarantees comparable to TLS and is faster in the normal case

CERIAS

PURDUE
UNIVERSITY