NDS2

Network and Distributed Systems Security

Towards a faster and more secure web

Comparing QUIC to TCP Fast Open, TLS False Start, and TLS 1.3

Matthew Jagielski, Samuel Jero, Robert Lychev, Alexandra Boldyreva, and Cristina Nita-Rotaru

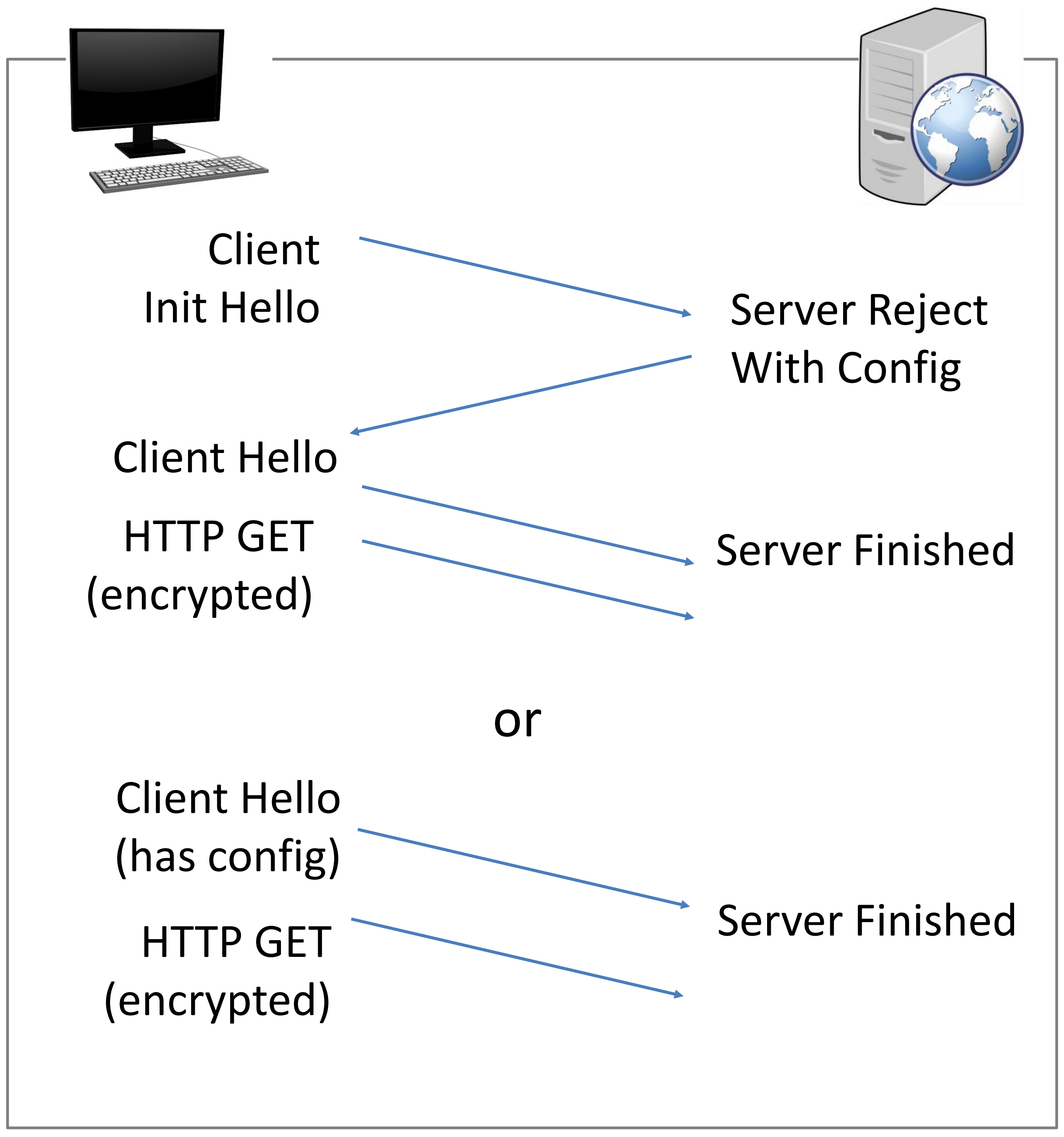
QUIC

Authenticate and encrypt connection

Reduce latency (1- or even 0-RTT)

Two phase key exchange

Made by Google for Chrome



QUIC Initial Key Exchange

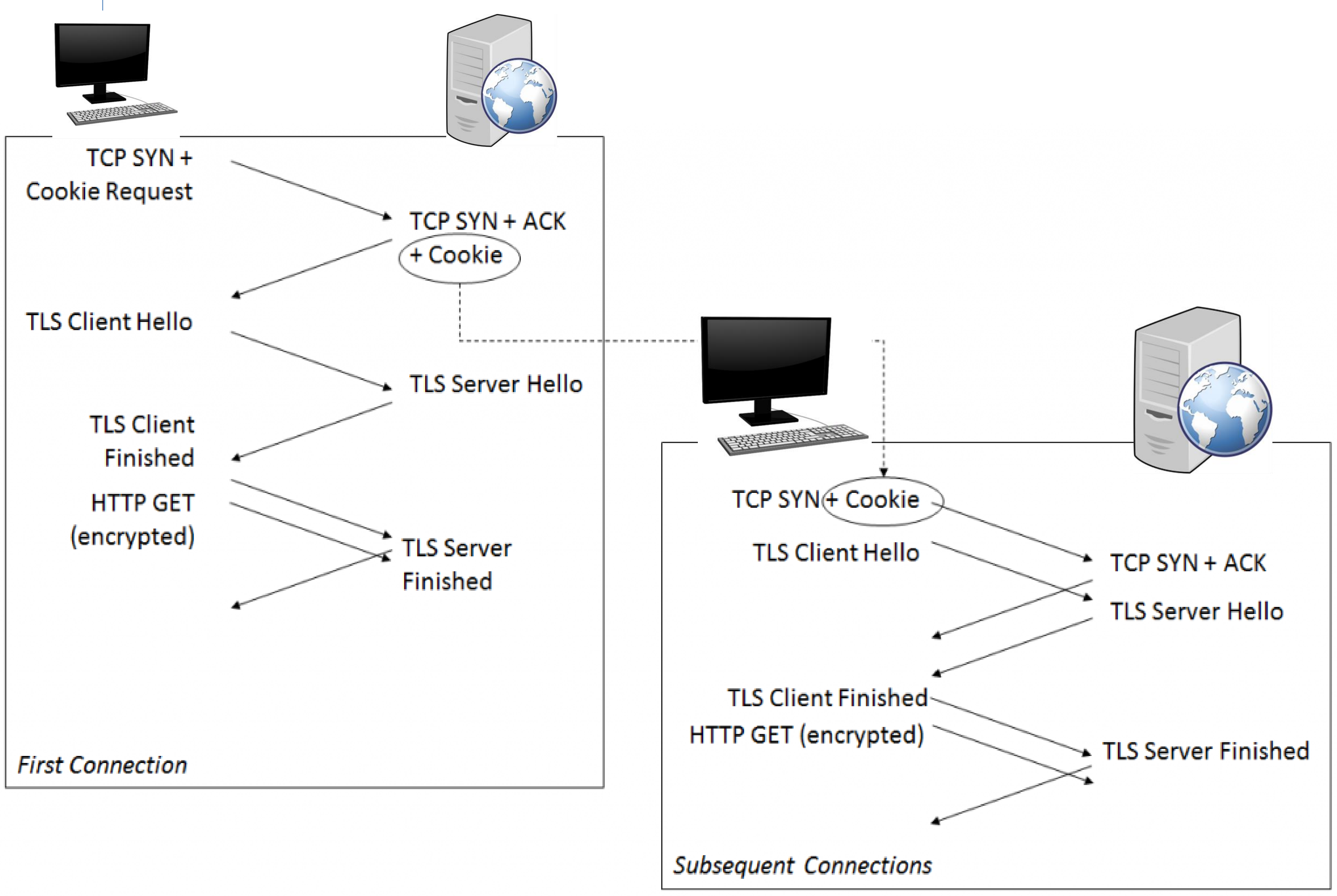
TCP Fast Open and TLS False Start

Also authenticate and encrypt a connection

Similar latency promises

Key exchange complete after first phase

Provided optionally by several browsers



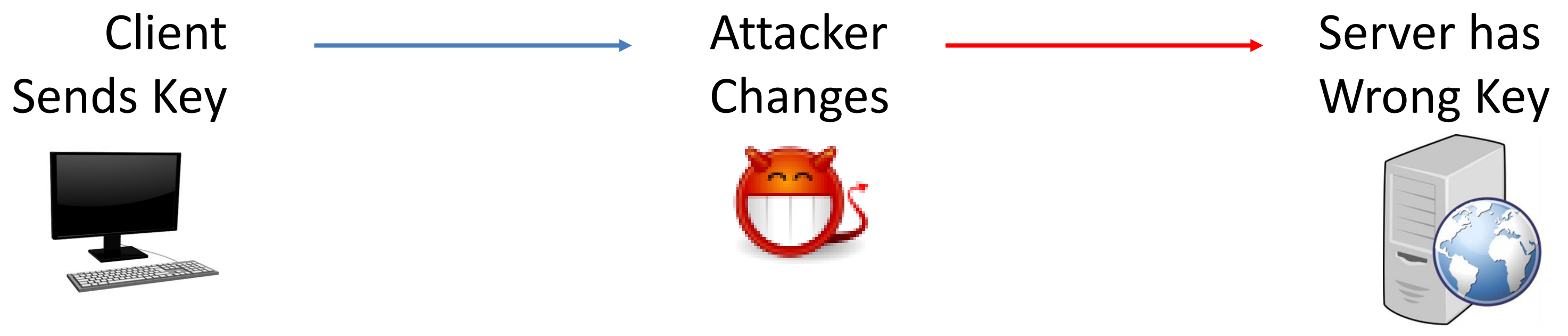
TCP Fast Open + TLS False Start Key Exchange

QUIC Analysis

- New security model made for QUIC –

  Security for two phase key exchange
- Prove security by reduction to cryptographic assumptions -

  Signature scheme, encryption scheme, and key exchange security
- Performance attacks demonstrated on QUIC –



Future Research

Analyze these properties for TCP Fast Open + TLS False Start:

Can security be demonstrated under existing security models?

Is this network protocol secure, provided its cryptographic assumptions hold?

Even if the security cannot be compromised, can the performance?

Northeastern University