How Secure and Quick is QUIC In Presence of Malice?

Alexandra Boldyreva
Georgia Tech

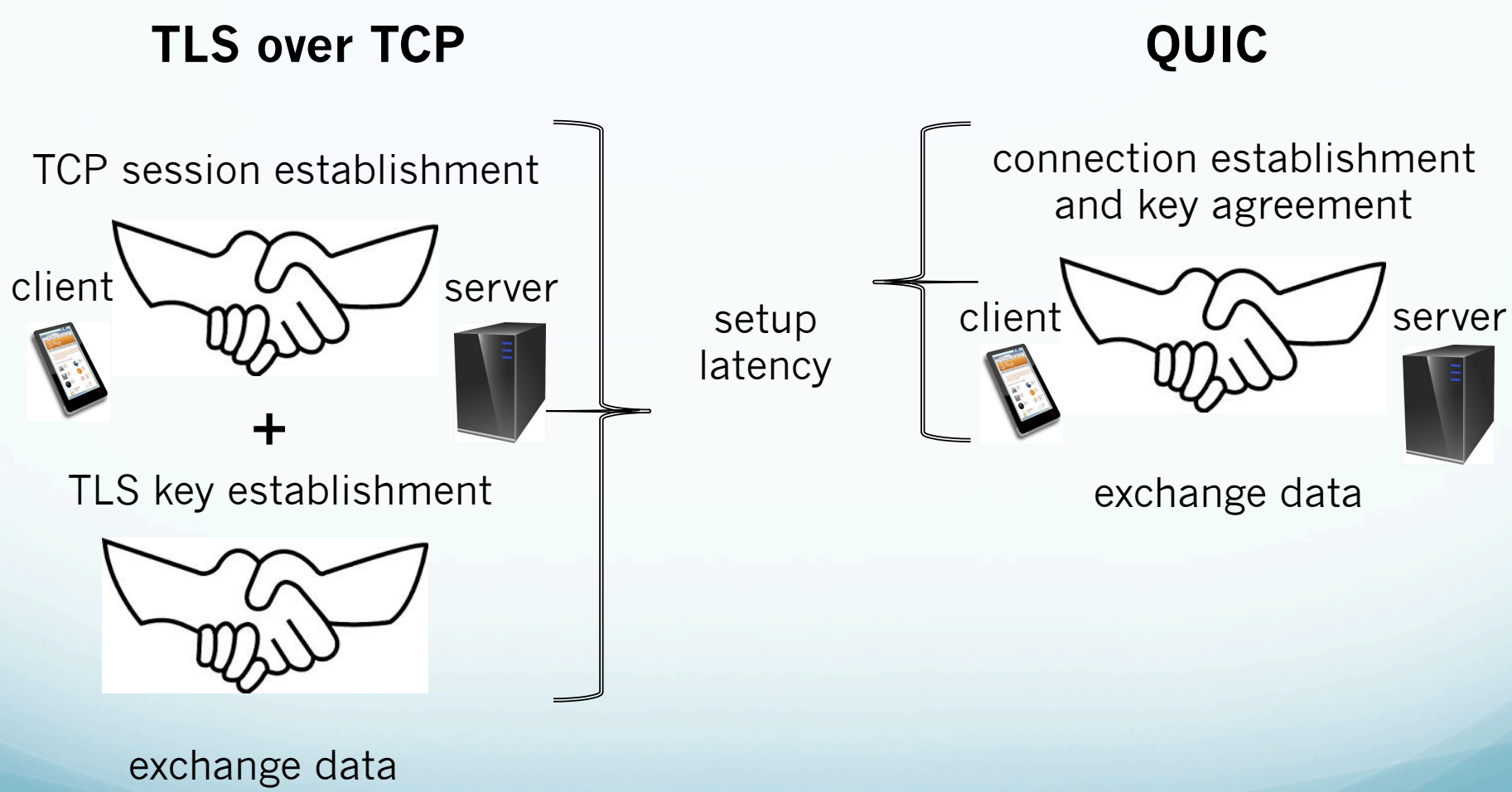
Robert Lychev
Georgia Tech

Cristina Nita-Rotaru
Purdue

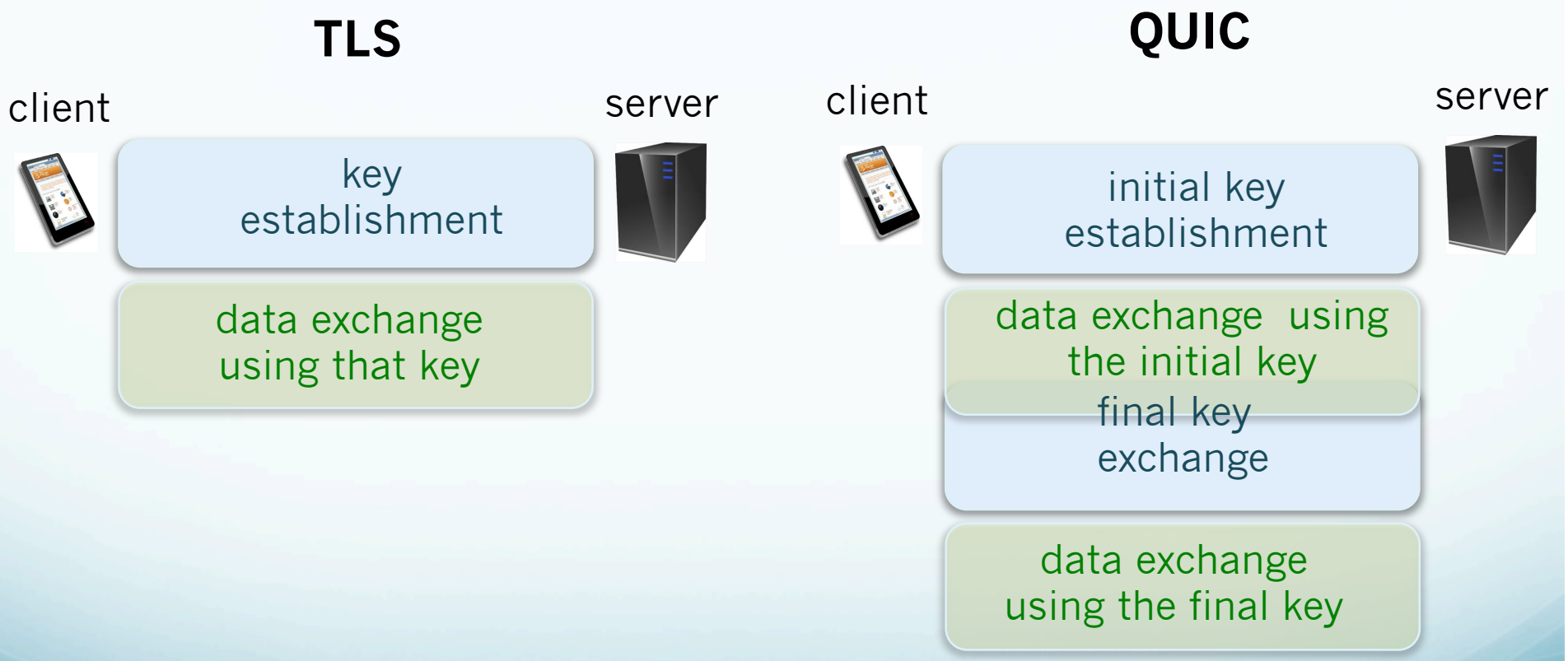
What Is QUIC?

- Stands for Quick UDP Internet Connections
- Communication protocol developed by Google and implemented as part of Chrome browser in 2013
- Was designed to
  - produce security protection comparable to TLS
  - reduce connection and transport latency

Setup Time in QUIC vs TLS



Starting Data Exchange in QUIC vs TLS



Our Main Questions

- What security guarantees does QUIC provide, and under which assumptions?
- How effective is QUIC at minimizing latency in presence of attackers?

Results Summary

- Existing security models (e.g., used to analyze TLS) are not suitable because in QUIC data can be exchanged under the initial key before the session key is set
- Thus, we develop a new security model
- We prove that QUIC meets security definition under reasonable assumptions
- However, simple but subtle manipulation attacks can introduce substantial latencies

Concurrent & Independent Work

Fischlin & Gunther CCS'14	Our work
• Analyze only QUIC's key agreement • Develop a security notion for multi-stage key agreement composable with any secure data exchange protocol • Prove QUIC's key exchange with a modification is secure • But what about the security of the whole protocol as is?	• We show that QUIC's cryptographic core (as is) is secure • Our model takes into account IP-spoofing attacks • We analyze QUIC's latency guarantees in presence of attackers

Thank You

Paper to be posted soon on e-print.