Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

16th September 2019
Elbsides 2019

Improving the Privacy of TCP Fast Open, TLS 1.3 and QUIC

Erik Sy

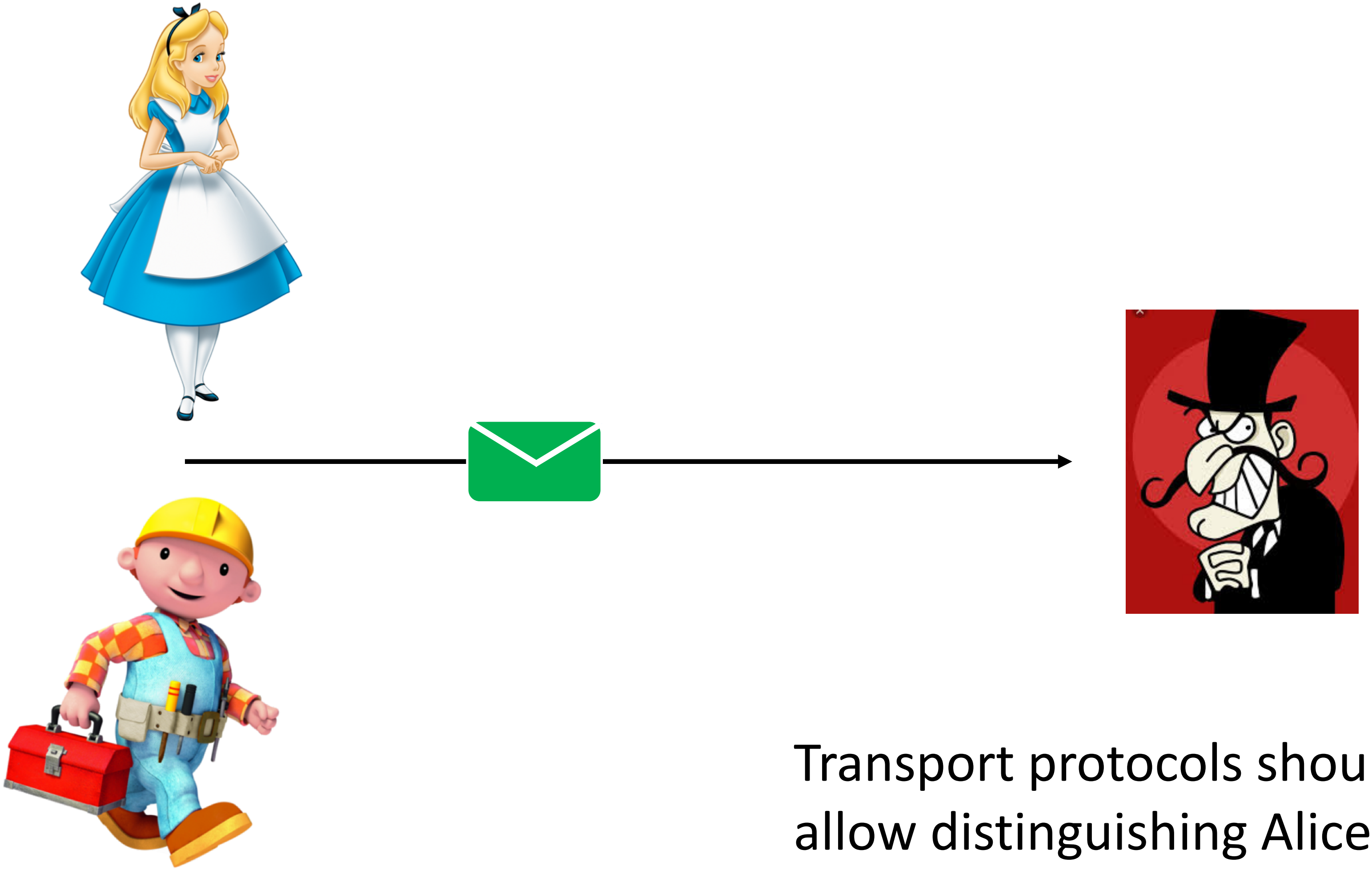
The Right to Informational Self-Determination

- Individuals have the right to determine in principle the disclosure and use of their personal data (German constitution)
- “Self-determination is an elementary prerequisite for the functioning of a free democratic society” (Census Act, German Federal Constitutional Court)

Picture: dpa

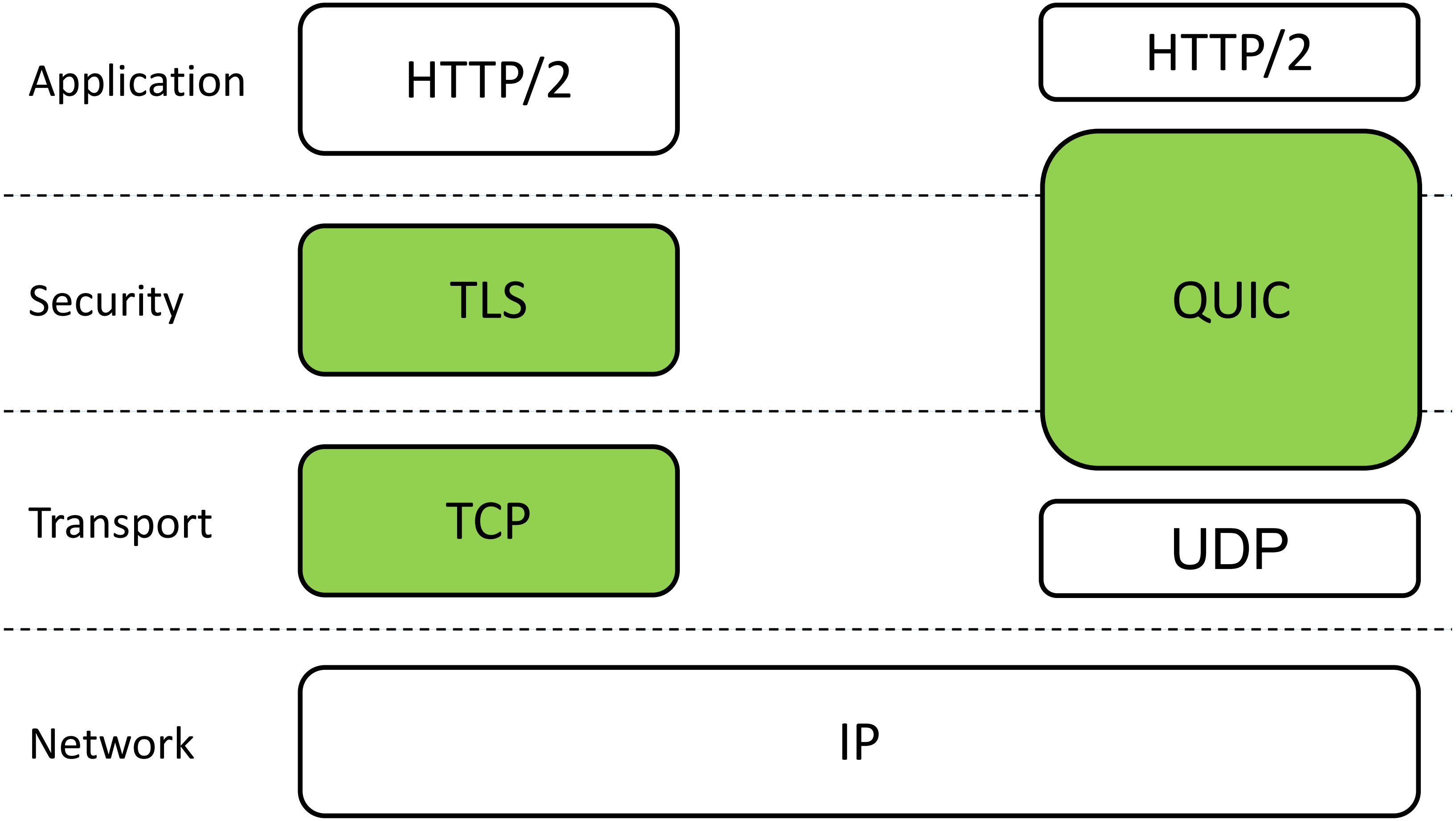
Do core Internet protocols comply with our right to informational self-determination?

Motivation



Transport protocols should not allow distinguishing Alice and Bob as the sender of a message.

Investigated Protocols



Application

HTTP/2

HTTP/2

Security

TLS

QUIC

Transport

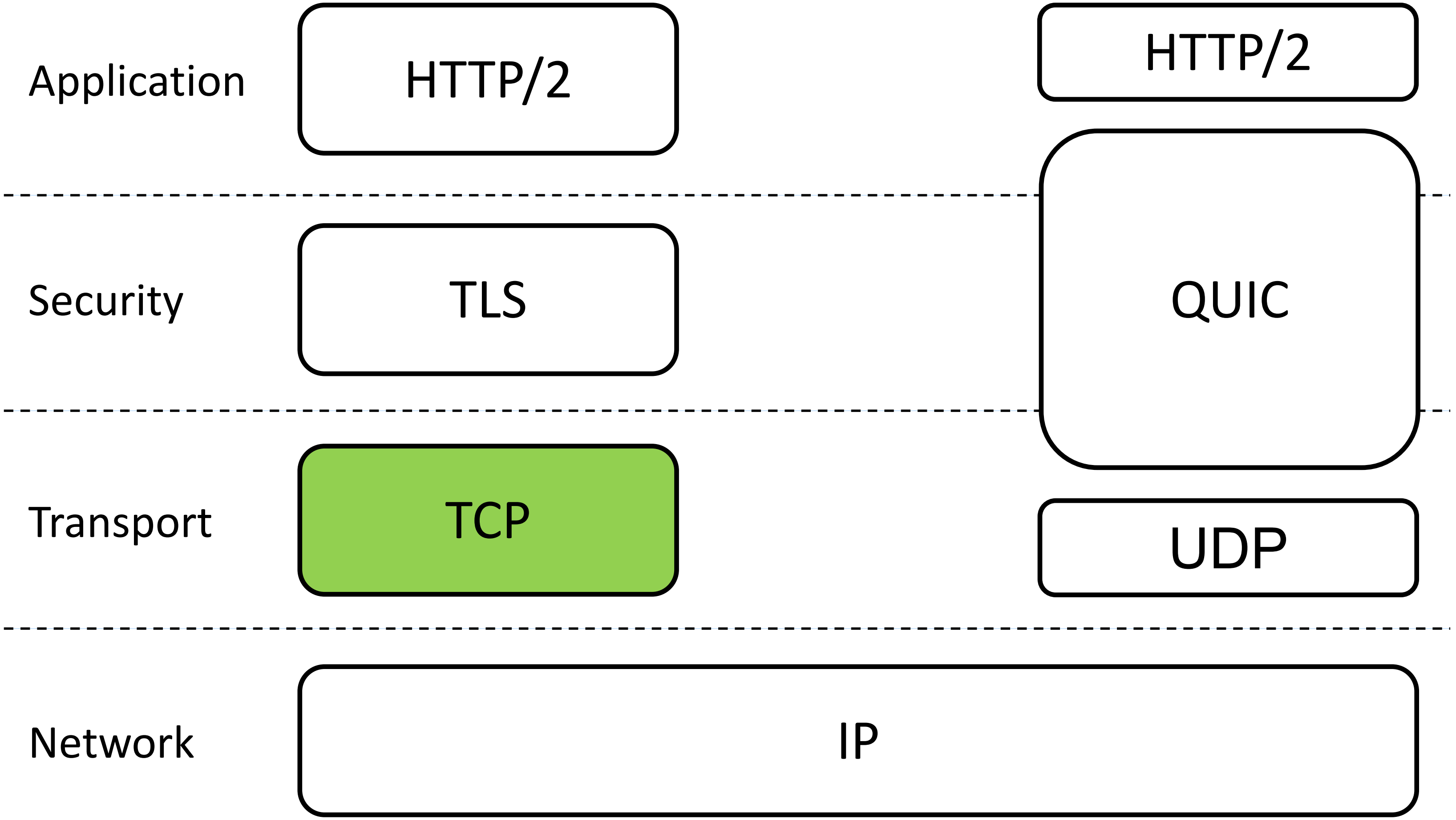
TCP

UDP

Network

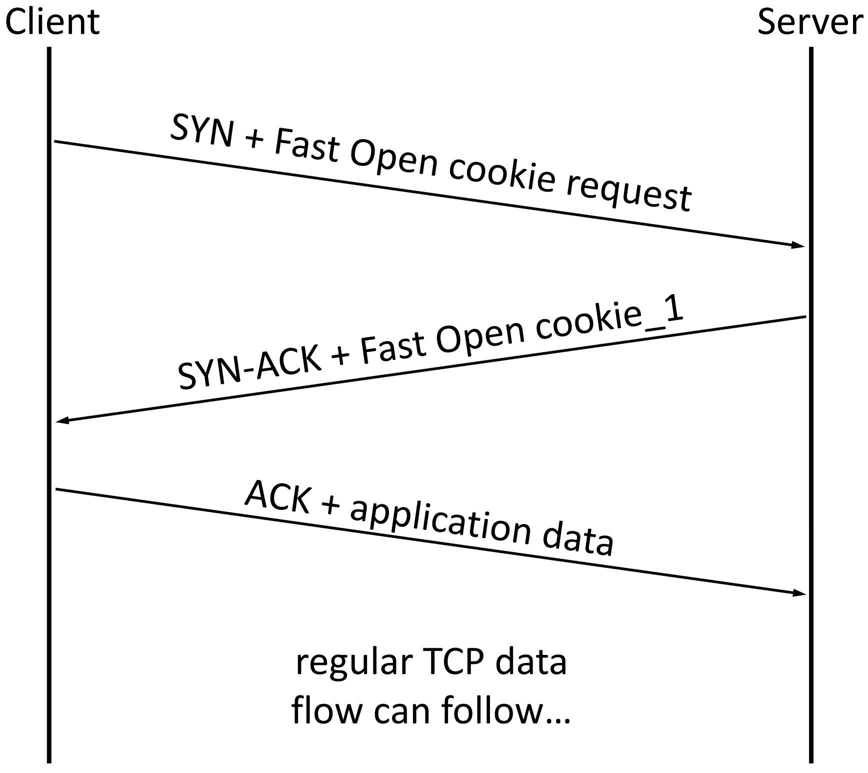
IP

Introducing TCP Fast Open (RFC 7413, Dec 2014)

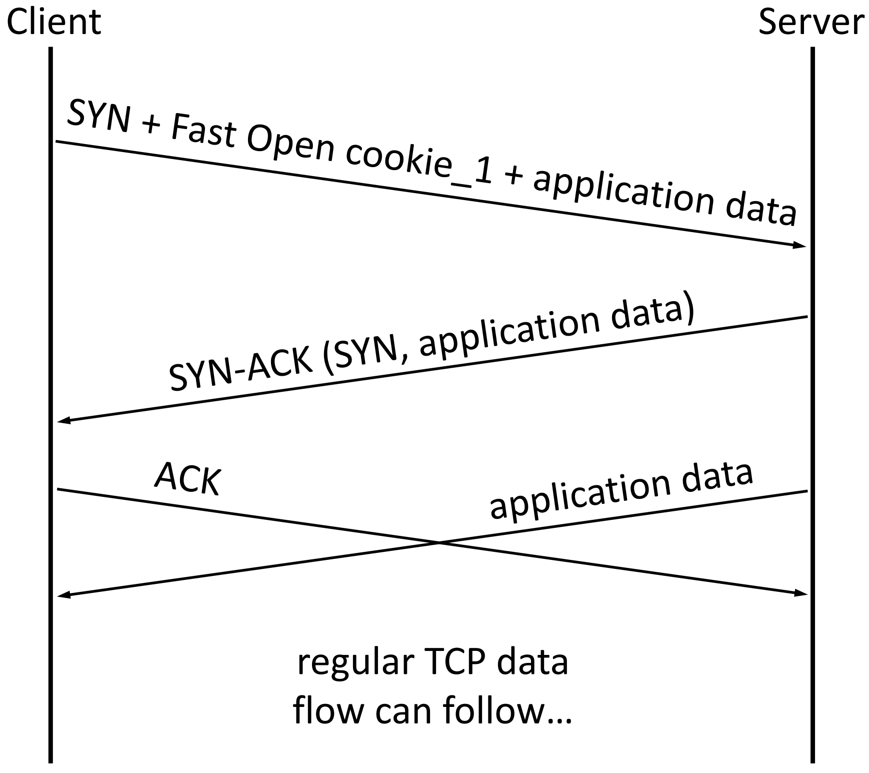


Introducing TCP Fast Open (RFC 7413)

- Allows validating the client's IP address without an additional round trip



1) Initial handshake


Client
Server
SYN + Fast Open cookie_1 + application data
SYN-ACK (SYN, application data)
ACK
application data
regular TCP data
flow can follow…

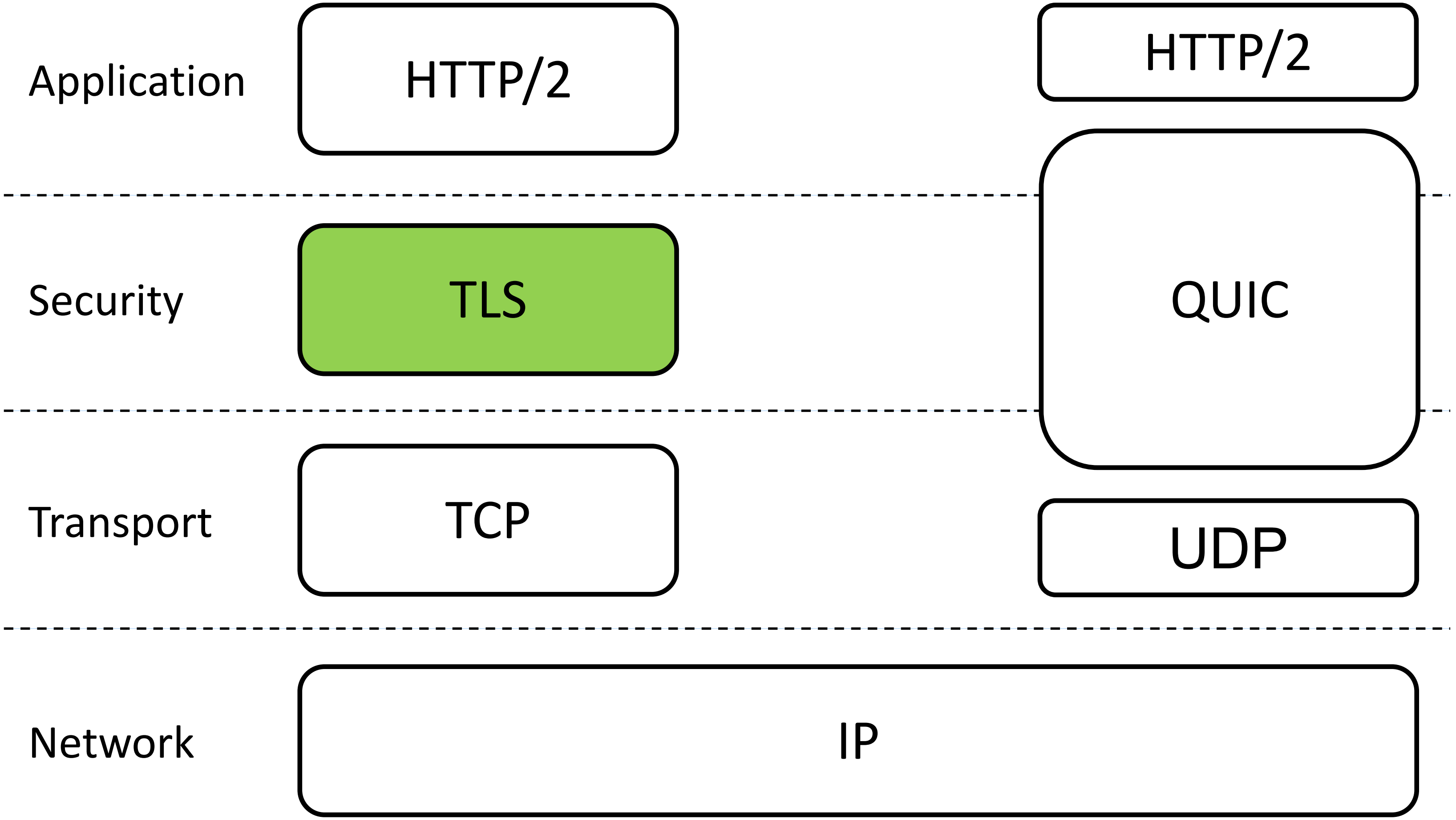
2) Abbreviated handshake

User Tracking via TCP Fast Open

- Main findings[1]
  - Fast Open cookies present a kernel-based tracking mechanism
  - Tracking feasible for network observer
  - Feasible tracking periods are unrestricted
  - Enables tracking across private browsing modes, browser restarts, and different applications
- Reactions by browser vendors
  - Mozilla stopped using TFO within Firefox
  - Microsoft stopped using TFO within the private browsing mode of Edge

[1] Sy et al. “Enhanced Performance and Privacy for TLS over TCP Fast Open” (2019)

Introducing TLS Session Resumption

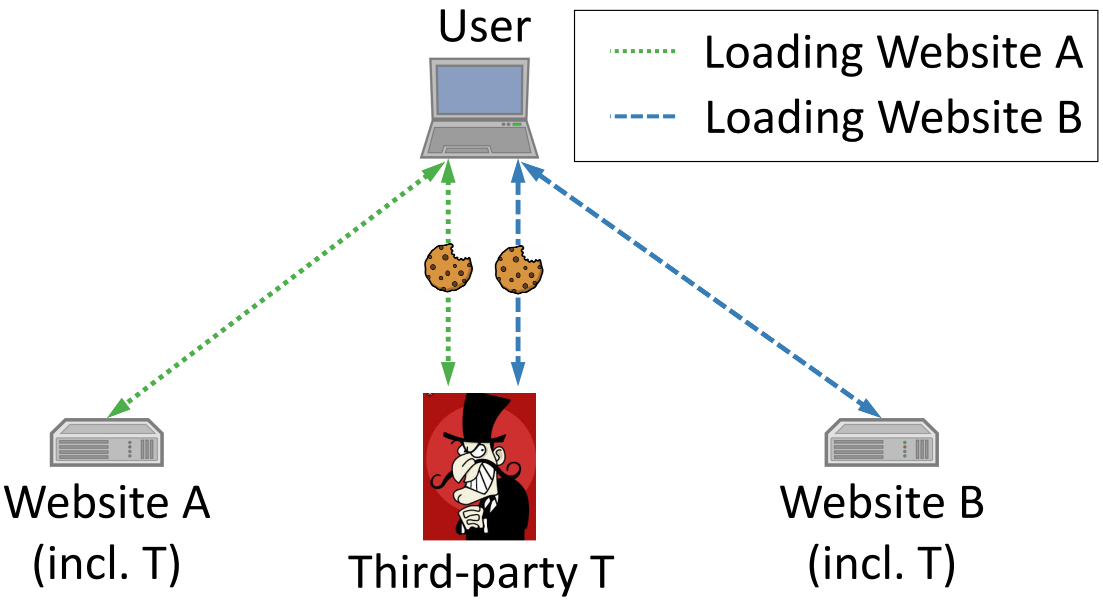


Introduction to TLS Session Resumption

- Allows a client-server pair to establish a new TLS connection with a previously exchanged symmetric key
  - Reduces the delay and the computational overhead of TLS handshakes
  - Server can uniquely identify clients based on this secret key
- Deployment on the Internet
  - 96% of TLS-enabled Alexa Top Million Sites support TLS resumption
  - All popular web browsers support this feature, which is included in every TLS version

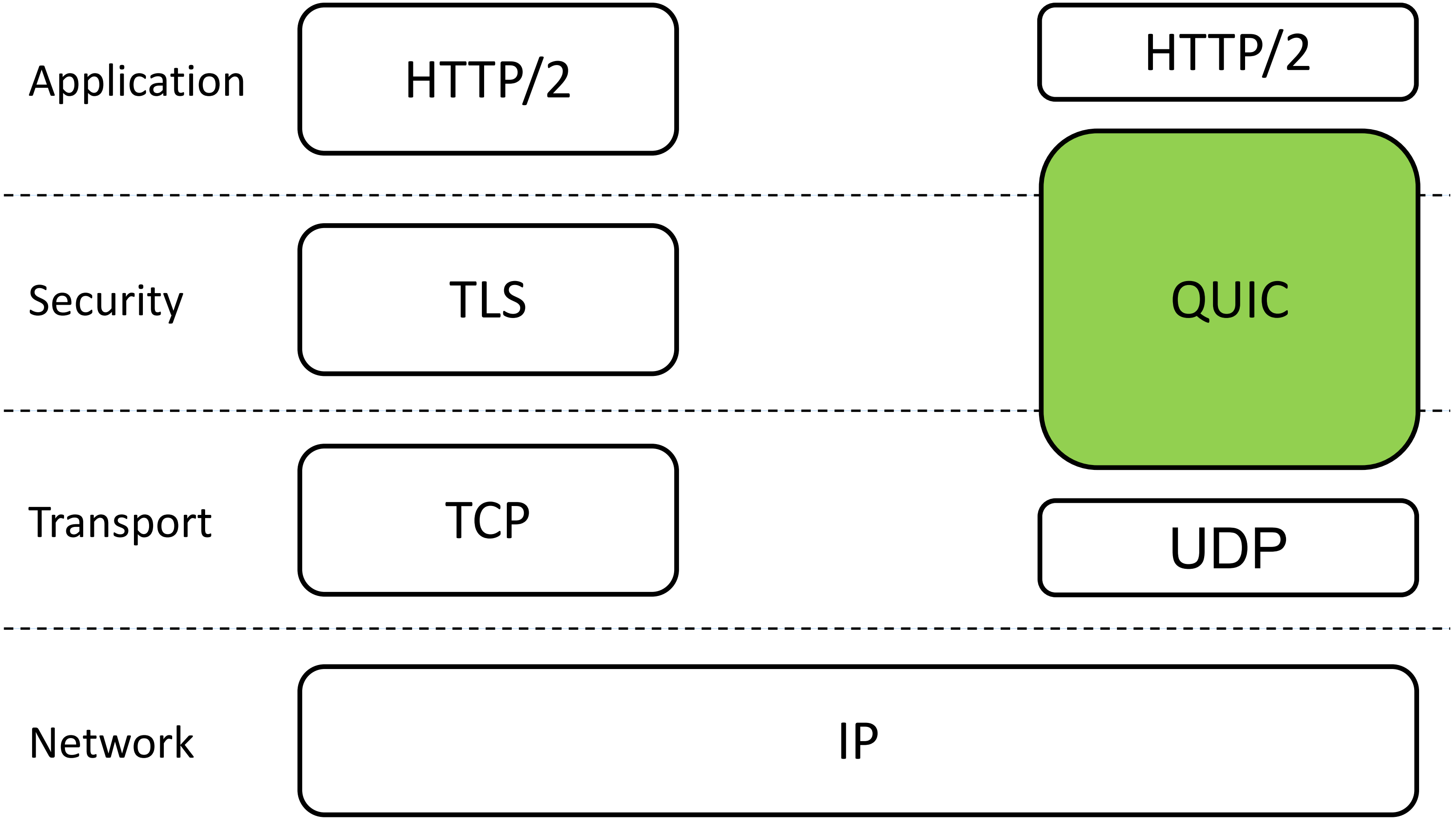
Tracking via TLS Session Resumption

- Main findings[2]
  - Safari and Firefox can be tracked for at least 24h using this mechanism
  - Prolongation attack extends feasible tracking periods
  - Only TLS v1.3 protects against tracking by network observer
  - Most browsers do not protect against third-party tracking via TLS SR



[2] Sy et al. “Tracking Users across the Web via TLS Session Resumption” (2018)

Introducing QUIC



Introduction to the QUIC Transport Protocol

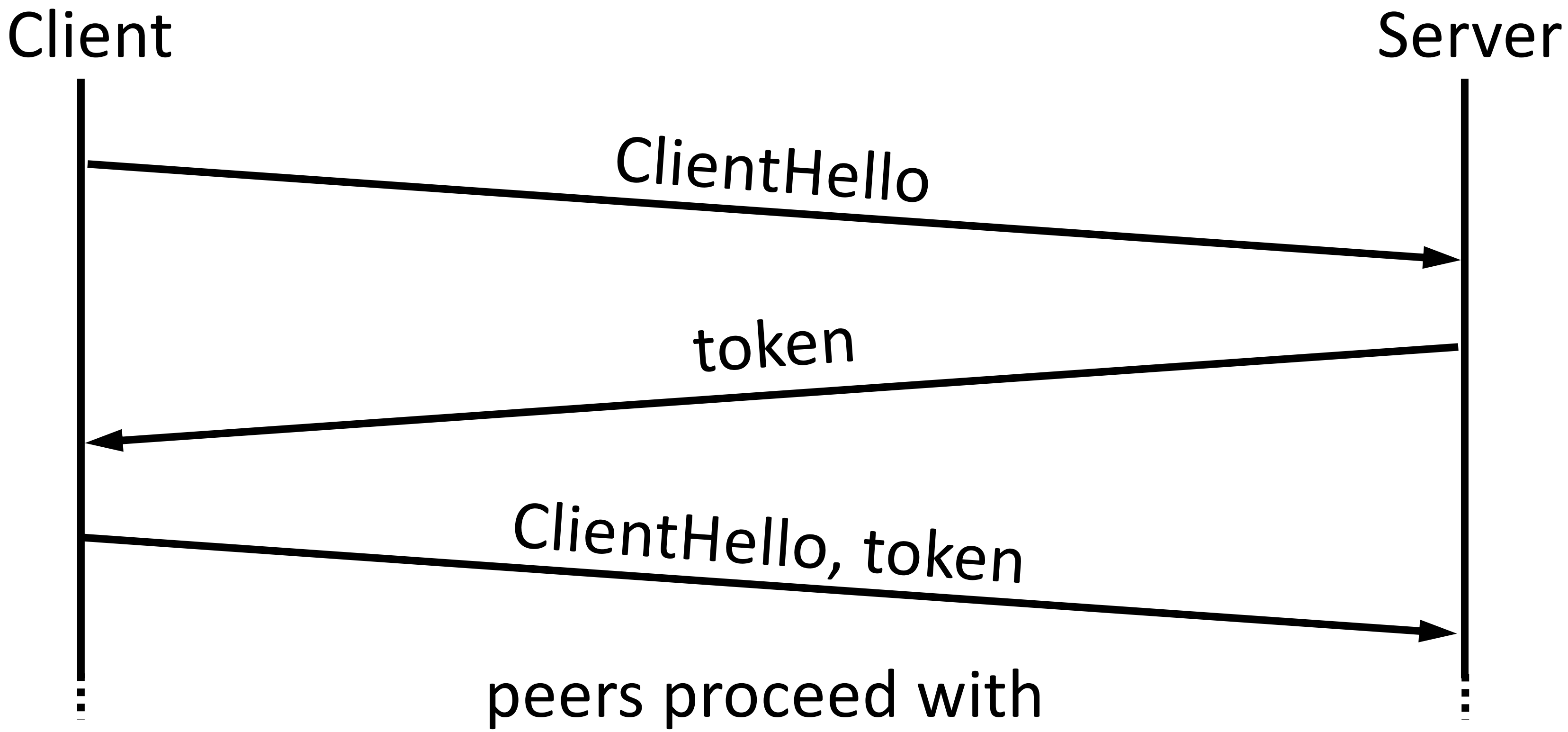
- QUIC is going to replace TLS over TCP in HTTP/3

- Improves problems of TLS over TCP
  - Protocol Entrenchment
  - Implementation Entrenchment
  - Handshake Delay
  - Head-of-line Blocking
  - Mobility

- Google’s QUIC protocol is already widely deployed on the Internet
  - Accounts for 7% of global Internet traffic
  - Supported by Google Chrome (approx. 60% browser market share)

Tracking via Source-Address Token

- Source-address token speed up the validation of the client’s IP address in subsequent connections between the same peers



Client

Server

ClientHello

token

ClientHello, token

peers proceed with connection establishment …

Tracking via QUIC’s Server Config

- QUIC’s server config contains a public key used to bootstrap the cryptographic connection establishment
- Client reuses server config across different connections
- Tracking feasible if server distributes unique server configs/ server config identifiers to its clients

Tracking via QUIC

- Main findings[3]
  - Default configuration of Chrome enables unlimited tracking periods
  - Third-party tracking feasible via this mechanism for Chrome
  - Network observers may track user’s via QUIC’s server config

- Reactions by browser vendors
  - Google Chrome restricts feasible tracking periods to one week

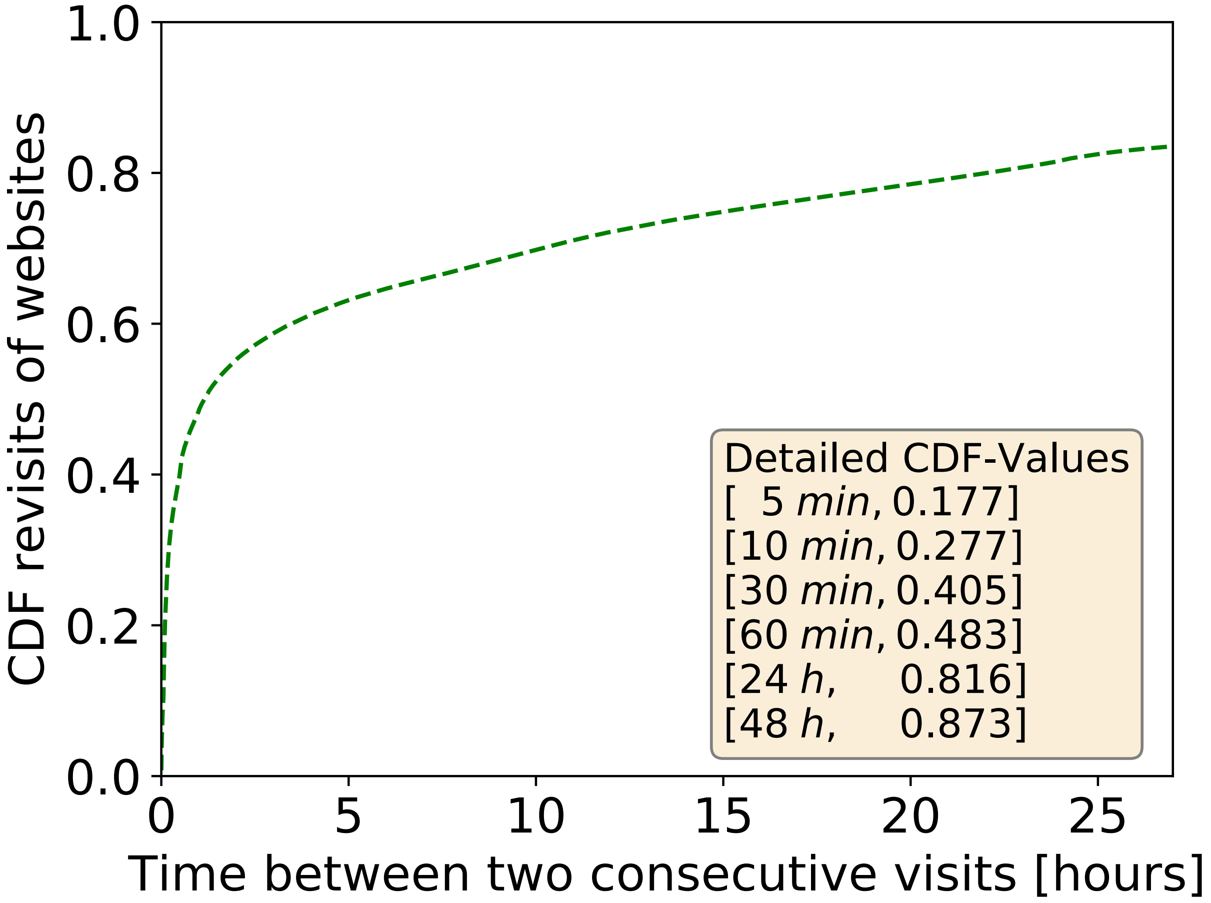
[3] Sy et al. “A QUIC Look at Web Tracking” (2019)

Recommended Privacy Protections

- Deactivate TCP Fast Open
- Applications restricting tracking via HTTP cookies should apply the same limitations to tracking via the presented mechanisms in TLS and QUIC

The Performance versus Privacy Trade-off

- Short lifetime for the investigated tracking mechanisms provides already significant performance gains while limiting feasible tracking periods



Detailed CDF-Values
[5 *min*, 0.177]
[10 *min*, 0.277]
[30 *min*, 0.405]
[60 *min*, 0.483]
[24 *h*, 0.816]
[48 *h*, 0.873]

Conclusion

- TCP Fast Open, TLS, and QUIC contain mechanisms that can severely harm the privacy of users

- Presented tracking mechanisms are stealthy compared to tracking via browser fingerprinting or HTTP cookies

- Popular browsers do not sufficiently protect against these privacy risks

- Investigated mechanisms should be used with a short expiration time to balance the performance versus privacy trade-off

Thank you

Questions and Answers

E-mail:	ElbSides@erik-sy.de
Slides:	https://erik-sy.de/elbsides