CS 925

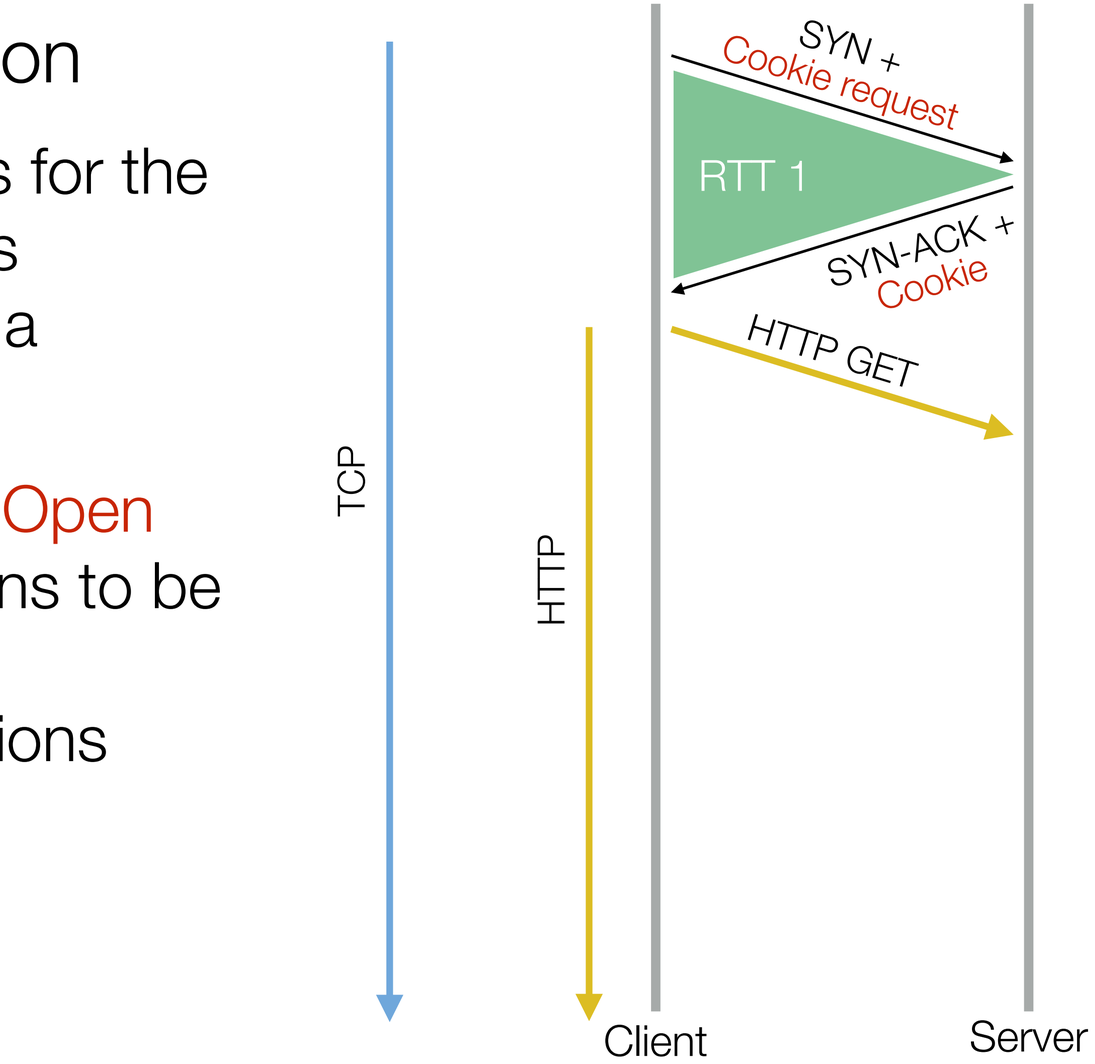
Lecture 13

Transport Protocol Evolution

Tuesday, March 5, 2024

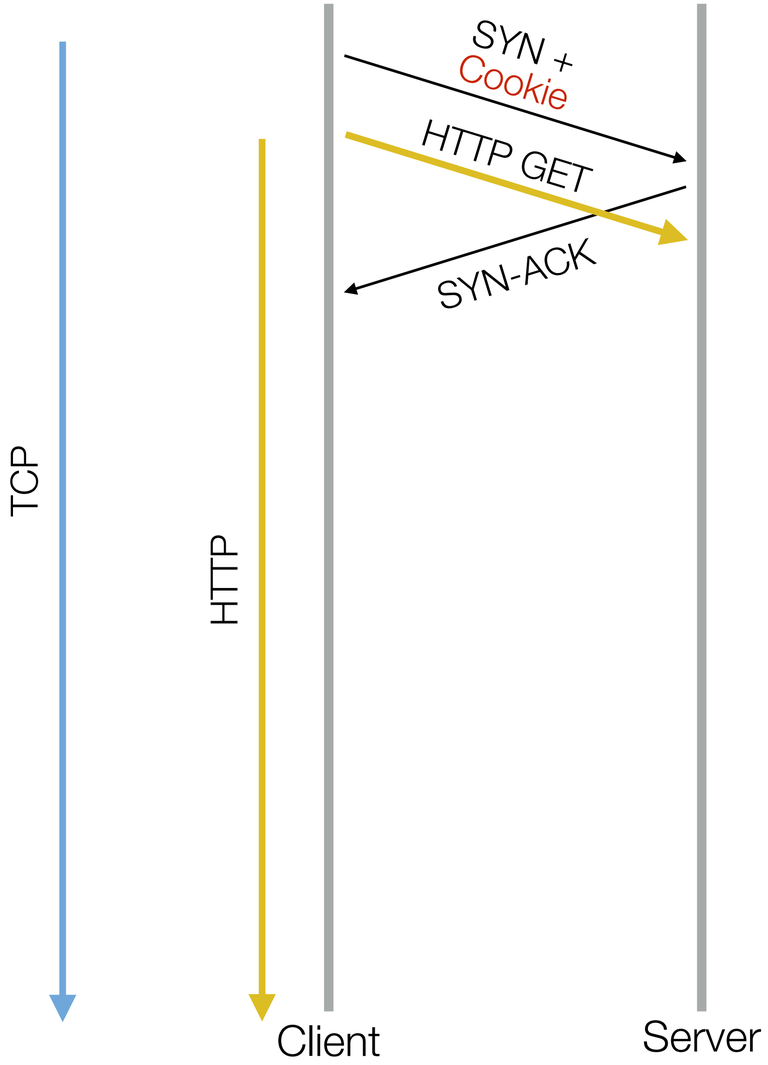
TCP Fast Open

- TCP Fast Open option
  - when client connects for the first time, one RTTs is required to establish a connection
  - server provides Fast Open Cookie in TCP Options to be used to speed-up subsequent connections



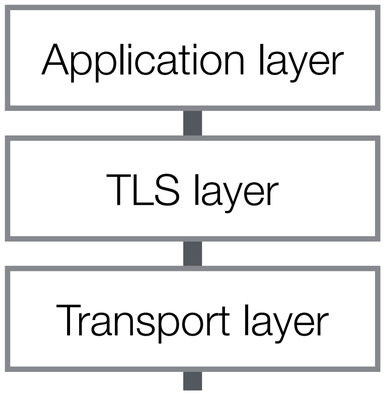
TCP Fast Open

- TCP Fast Open option
  - for subsequent connections, data can be immediately sent
  - client sends previously received Fast Open Cookie



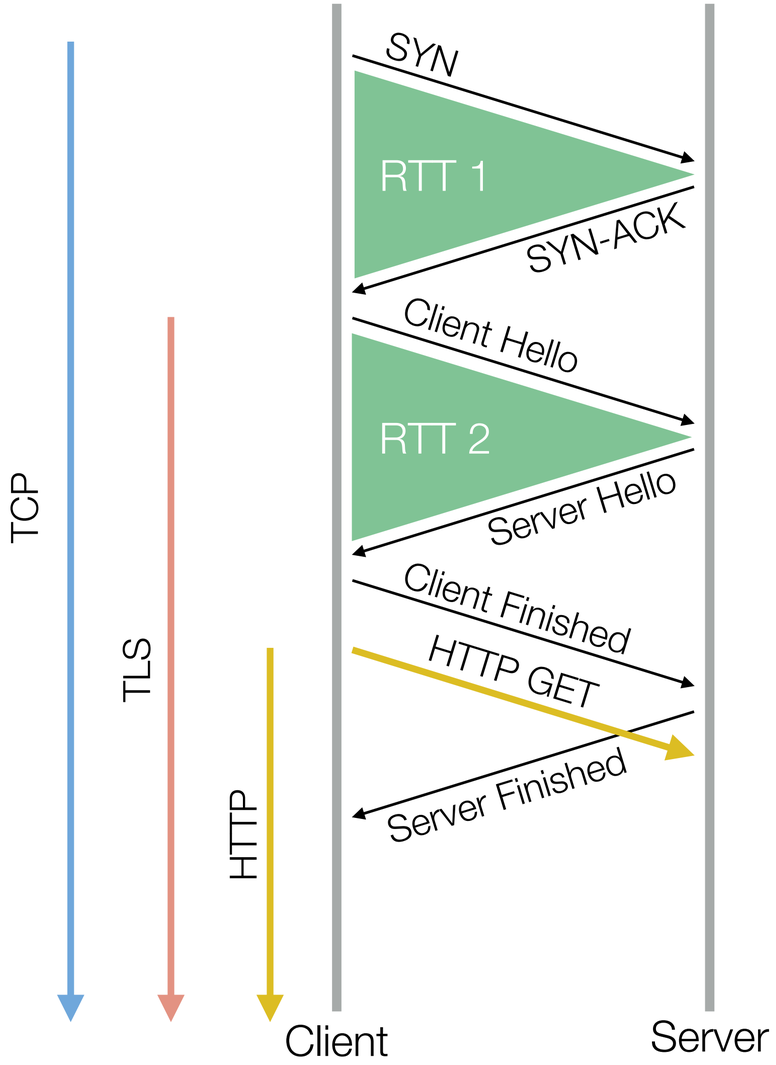
Transport Layer Security

- Transport Layer Security (TLS) - cryptographic protocols that to provide privacy (encryption) and data integrity protection
- … earlier versions known as SSL (Secure Socket Layer) is now deprecated but the term is widely used as a synonym for TLS
- Most used version TLS 1.2 (2008)
- Current version: TLS 1.3



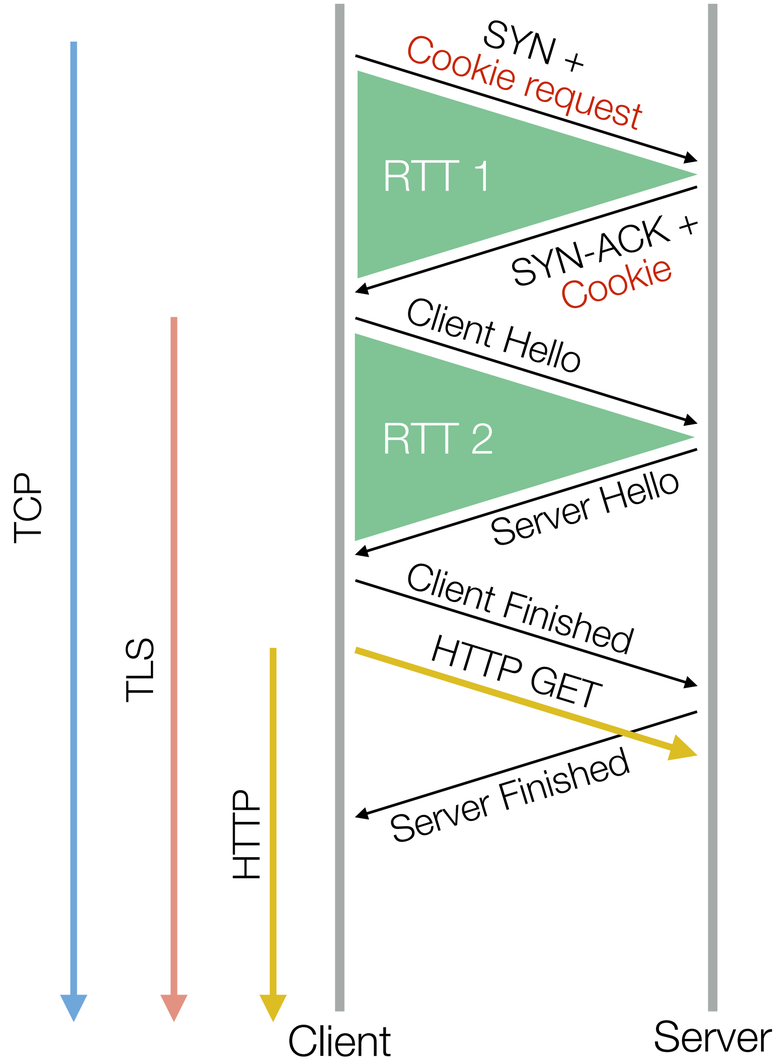
TLS connection latency

- TLS False Start option
  - for pre-TLS 1.3 versions
  - 2 RTTs required to establish a secure connection



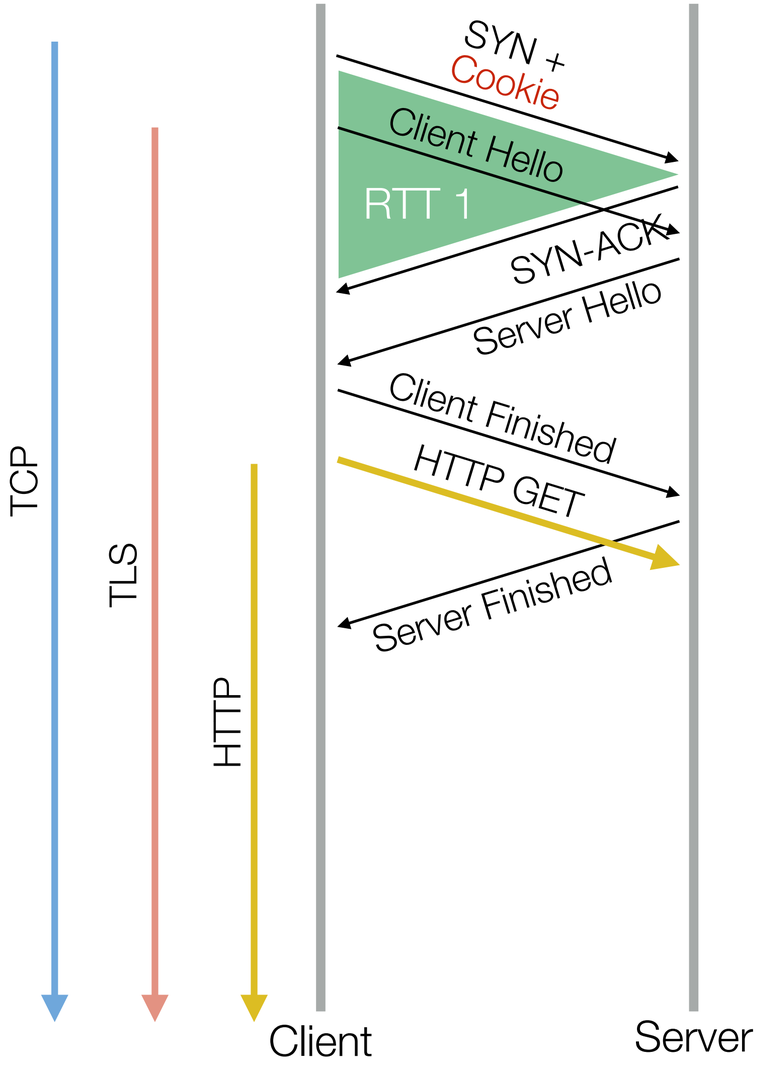
TLS connection latency

- with TCP Fast Open option
  - when client connects for the first time, 2 RTTs are still required to establish a secure connection
  - server provides Fast Open Cookie to be used to speed-up subsequent connections



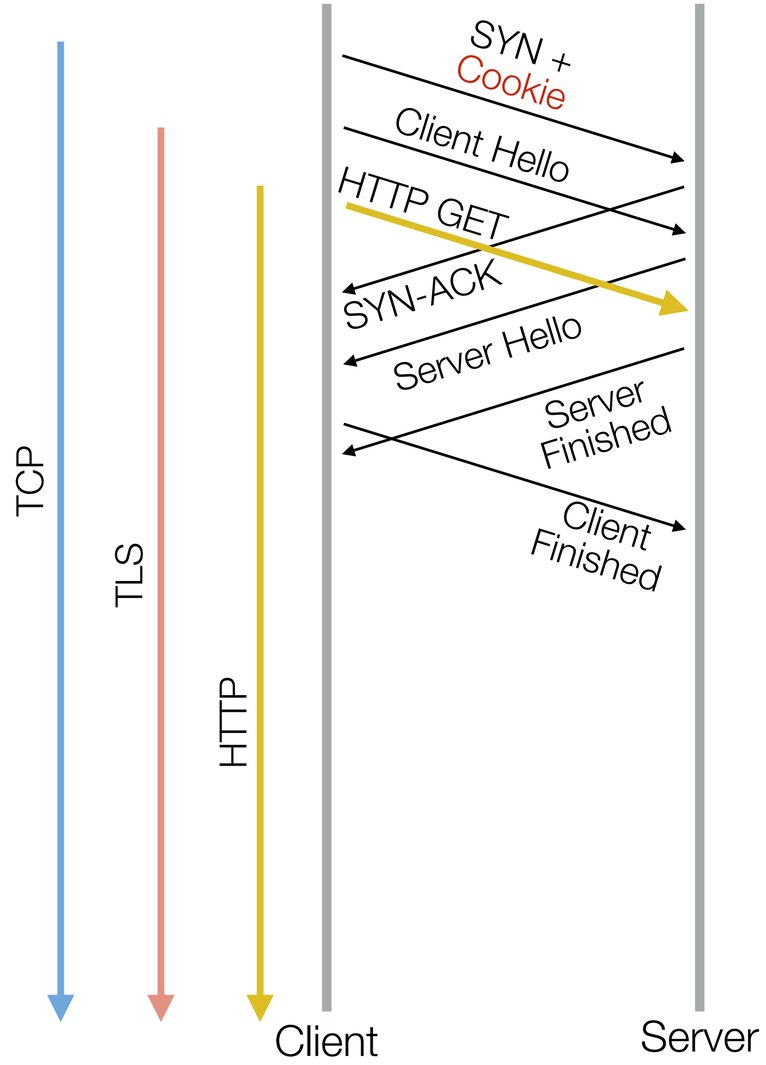
TLS connection latency

- with TCP Fast Open option
  - for subsequent connections, only one RTTs required to establish a secure connection
  - client sends previously received Fast Open Cookie



TLS connection latency

- 0-RTT with TLS 1.3
  - for subsequent connections (using Fast Open Cookie), HTTP command is set before the TLS connection is fully established
  - However, the initial data sent to the server is susceptible (e.g., replay attack)



SNI (Server Name Indication)

- Background: HTTP/1.1
  - Host: <hostname> header line indicates the visual host for which the request is sent
  - This does not work with TLS because the certificate is presented before HTTP headers are sent
- SNI (Server Name Indication)
  - TLS extension included in the handshake
  - Specifies the hostname (or domain name)
  - (reveals the requested server hostname to middle boxes)
- Encrypted SNI (ESNI)