TLS 1.3, 0-RTT, HTTP, and You

Eric Rescorla

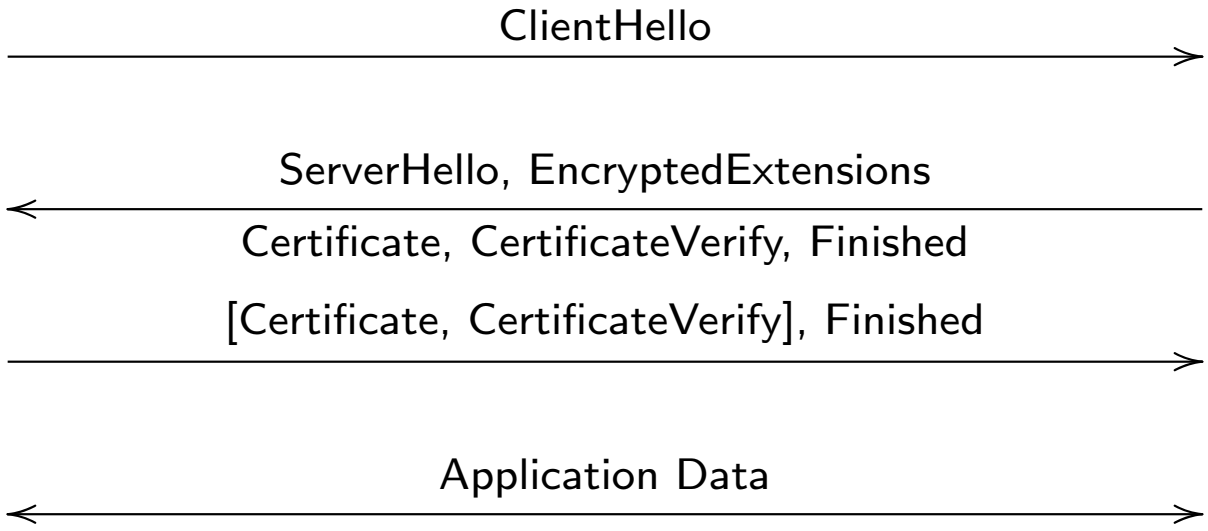
Mozilla

ekr@rtfm.com

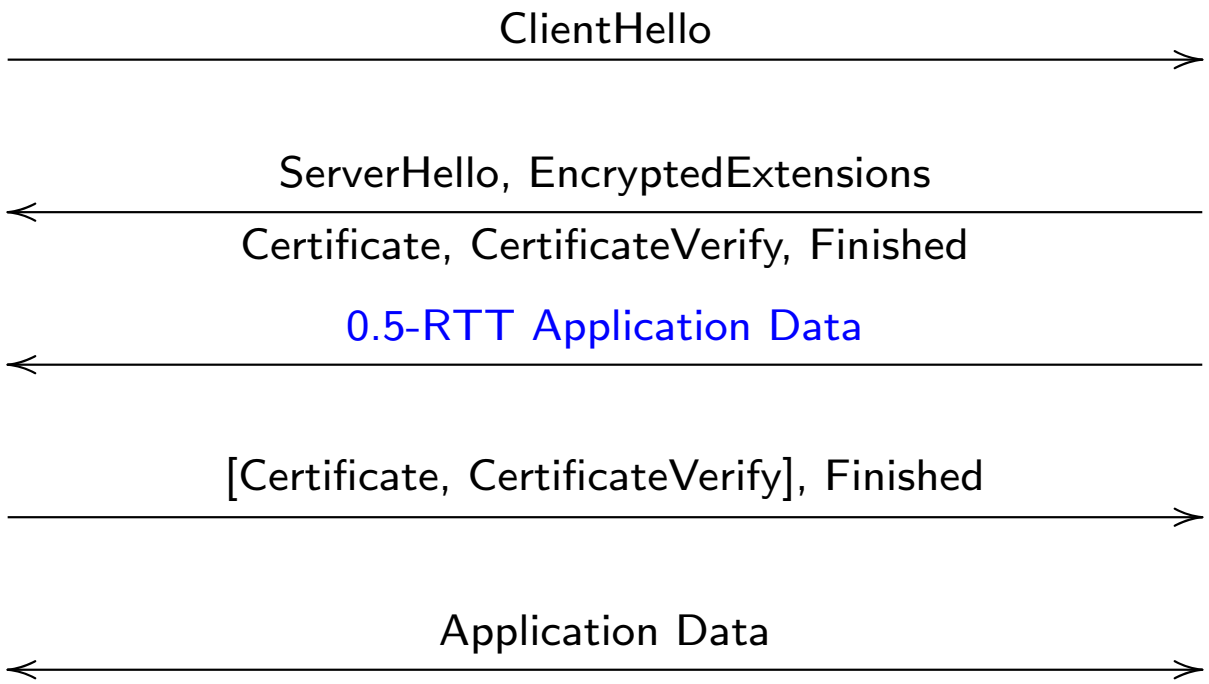
What you need to know about TLS 1.3

- Newest version of TLS – gradually rolling out
  - On by default in beta versions of Chrome, Firefox (and off by default in pre-release Safari), OpenSSL (some version diversity)
  - Already on on Cloudflare, Gmail, etc.
  - Some fighting with broken middleboxes
- A bunch of security improvements
  - Improved metadata resistance (encrypted certificates, optional padding feature, ...)
- Performance improvements (this is what you care about)
  - 0.5-RTT data (on servers first flight)
  - 0-RTT data (on clients first flight)

Basic TLS 1.3 Handshake



0.5 RTT Data


ClientHello
ServerHello, EncryptedExtensions
Certificate, CertificateVerify, Finished
0.5-RTT Application Data
[Certificate, CertificateVerify], Finished
Application Data

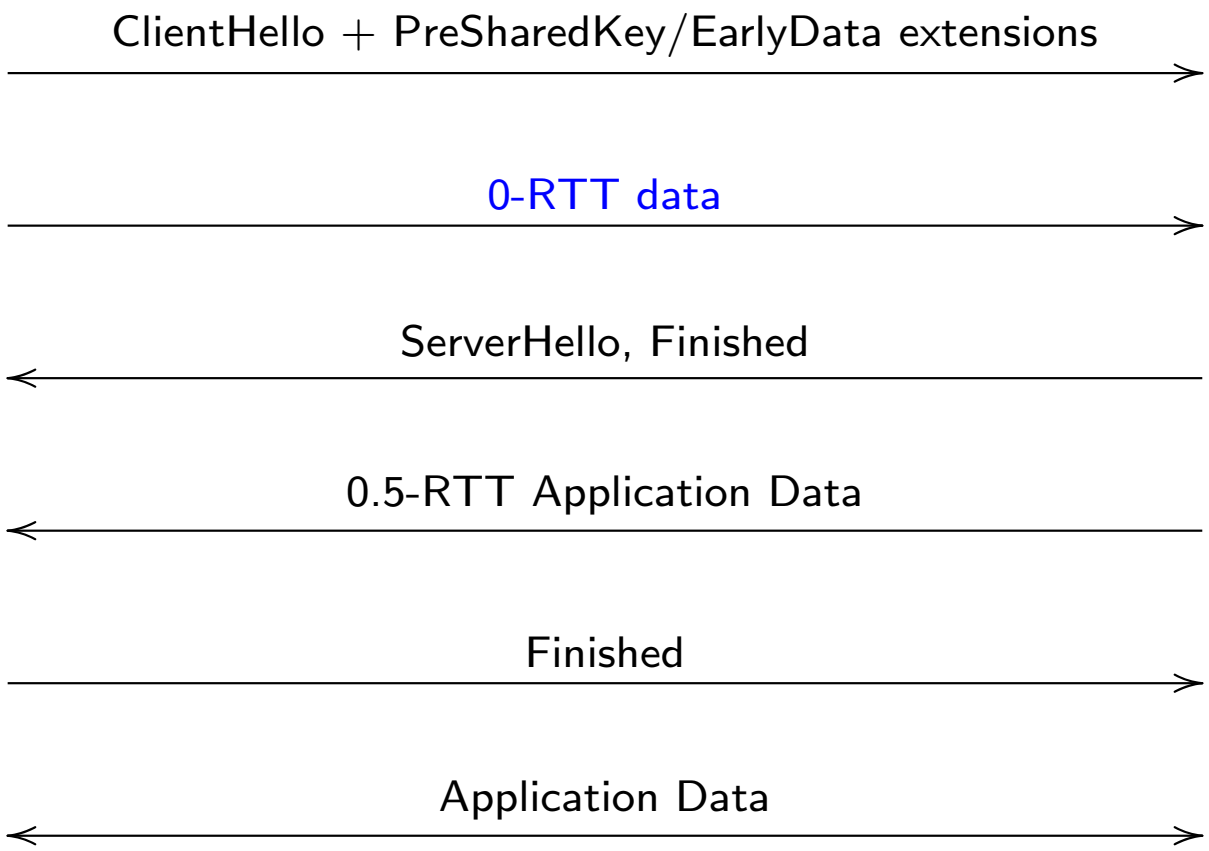
0.5-RTT Data Limitations

- Happens before client certificate
  - So clients are anonymous
  - ... unless they are resuming a client authenticated connection
- You don't know if the client is live
  - Attacker could just be sending a replayed ClientHello
  - More relevant for resumption

Potential 0.5-RTT Uses (HTTP)

- SETTINGs frames
- ORIGIN frame
- Auth certificate data
- Pushing commonly used data (e.g., `/index.html`)
- DNS priming

0-RTT


ClientHello + PreSharedKey/EarlyData extensions
0-RTT data
ServerHello, Finished
0.5-RTT Application Data
Finished
Application Data

0-RTT Data Limitations

- *Replayability*
  - Server can't be sure data isn't being replayed
  - Attacker can replay the early data
    - There are server-side defenses, but they are somewhat painful (sometimes nigh-impossible)
  - Many clients re-try (everything) on their own
  - Generally, clients and servers need to be careful here at the HTTP layer
- Not forward secure
  - At least when used with session tickets
  - Can use a session cache

    * But it's harder to build a distributed one

- No proof of liveness of client
  - (Related to the 0-RTT issue above).

0-RTT Uses

- First set of HTTP requests
- DNS (query goes in 0-RTT, response goes in 0.5 RTT)
- Everything else!

Questions/Discussion?