2 MYTHBUSTING HTTPS

GOOGLE I/O 2016

ISP or Wi-fi provider or some other intermediatory may inject obnoxious adds to the page.

↳ interferes with user experience

HTTPS → Data is protected from snooping and tampering.

https://

IDENTITY

→ Cryptographic proof of identity "certificate"

CONFIDENTIALITY

→ Only sender and receiver can read the data.

INTEGRITY

→ Intermediary can't modify and tamper the data.

① Use HTTPS even when website does not exchange any private content.

REASON : * Website becomes fast and reliable

* Access to strong APIs like GEOLOCATION ↓ restricted to safe browsing

⇒ Many APIs are restricted to HTTPS.

② NETWORK LATENCY

① HTTP to HTTPS redirects

② Setting up a TLS connection
↓
requires 2 Round trip times.

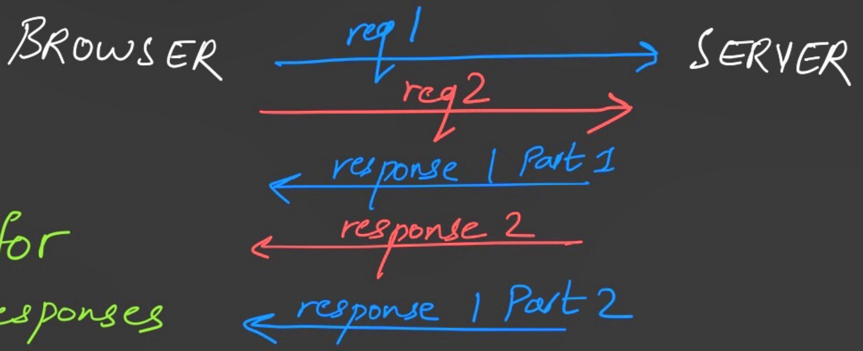
SOLUTION :

* HTTP Strict Transport Security
→ browser directly changes http to https until header expires.
⇒ ONLY 1 REDIRECT

* 1 TLS RTT can be prevented. Client can send HTTPS request before entire process completes.
⇒ TLS False Start → server starts processing before TLS completion

* Past sessions can be remembered by the server. Need not do entire TLS handshake again
⇒ TLS Session Resumption → Saves 1 RTT

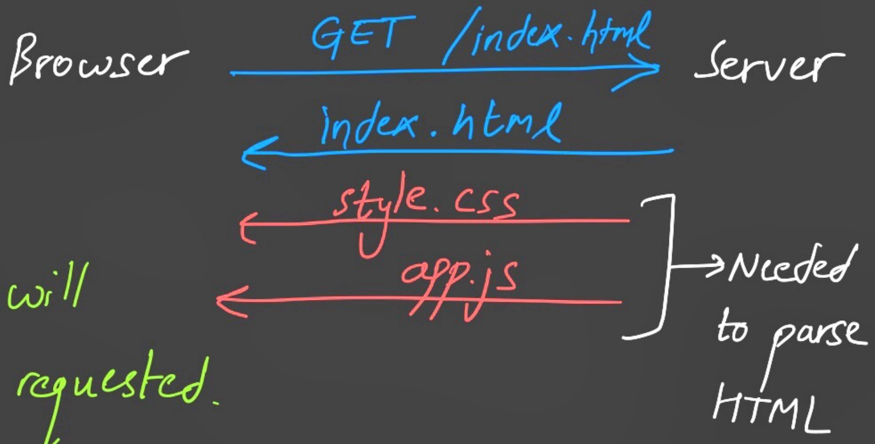
HTTP/2



① Multiplexing

use same connection for multiple requests and responses

② Server Push



Proactively push the requests that client will need before they are requested.

- ☆ Browsers only support HTTP/2 over HTTPS
  - ↳ intermediaries may break HTTP/2 because HTTP/2 traffic is different from HTTP.