Client Hints

IETF 104 - HTTPWG

@yoavweiss

Privacy Preserving Proactive Content Negotiation

- Server opt-in
  - Prevents passive fingerprinting
- Secure connection only
  - Prevents MITM extraction
- Same-origin only
  - Prevents unauthorized fingerprinting by third parties
- Cross-origin delegation
  - Enables constrained third party legitimate uses

Opt-in mechanisms

- `Accept-CH`
  - Opt in for current navigation
- `Accept-CH-Lifetime`
  - Cached opt in for the origin

Third party delegation

- CH sent only on same-origin by default
  - Prevents information leaks through passive resources
- Delegated to 3P using Feature Policy
  - E.g. `Feature-Policy: ch-example ‘self’ foobar.com`

`Sec-` Prefix

- Prevent legacy servers bugs
- Enables to avoid CORS preflights
- May enable simpler processing in Fetch

Improved content negotiation

- Image-related hints - HTML PR
  - DPR
  - Viewport-Width
  - Width
- Network hints - NetInfo
  - RTT
  - Downlink
  - ECT
  - Save-Data
- Shipped in Chromium

Reduce passive fingerprinting surface

- Replace `User-Agent` and `Accept-Language` with CH
  - ua-client-hints and lang-client-hint
- Implemented in Chromium (but not shipped)

Changes to the draft

- Removed image-specific hints from it to reduce confusion
  - Hints using infrastructure defined in own specifications
  - Adopting infrastructure does not imply adopting all features
- PRing `Sec-` prefix recommendation
- Overall specification situation: bit.ly/client-hints-spec

Looking for more implementers

- We have running code in Chromium and servers
- Want more browsers to implement
  - To move forward IETF draft
  - To land Fetch and HTML PRs
  - To improve user privacy and experience