draft-hodges-websec-framework-reqs-00

Jeff “=JeffH” Hodges

IETF-81

Quebec City, Canada

Present Status

- `draft-hodges-websec-framework-reqs-00` submitted on 7-Mar-2011
- Brand new
- Very rough
- Attempts to broad-brush sketch overall Web Application problem space
- Leverages Content Security Policy discussion from public-web-security@w3.org list

Relevance Example

- Adam Langley (Chrome TLS/SSL implementer) noted on DANE list..
  - In message entitled “A browser's myopic view” (Sat, 9 Apr 2011 17:12:01 -0400 (14:12 PDT))
    - Noted that Chrome is only willing to have “hard fail” behavior (in forseeable future) wrt policy conveyed in the HTTP channel
    - Due to Secure DNS “last mile” issues
- This begs questions w.r.t. more general policy conveyance for Web Apps

Questions being Begged

- If Web Browsers are only willing to strictly enforce (for foreseeable future) policies conveyed in HTTP channel, e.g. HSTS, CSP
- And, if we anticipate policies such as LockFoo being desired by web apps who *may or may not* wish to declare the STS policy,
- Then do we need to invent yet another policy header to convey them?
  - Also begs question of needing to specify how policies conveyed in HTTP channel are combined and/or conflicts resolved

Further Impetus

- Thomas Roessler related a few minutes ago that he is aware of at least five other web app spec efforts that are now inventing HTTP headers for policy conveyance
  - “They're sprouting up all over the place...”

To Do

- Revise I-D
  - i.e. turn captured email threads into spec prose
  - Need review to help determine if all aspects of problem space are represented
  - Point to emerging other HTTP-conveyed web app policies being invented (? need pointers here)