draft-hodges-websec-framework-reqs

Jeff “=JeffH” Hodges
IETF-85
Atlanta, Georgia, US

Present Status

- **`draft-hodges-websec-framework-reqs-00`** originally submitted Mar-2011
- At -02 now, minor revisions to keep alive
- Very rough
- Attempts to broad-brush sketch overall Web Application problem space
- Leverages (early) 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, Public-Key-Pins
- Some policies desired by web apps *may or may not* be declared in conjunction with existing policies (see list above)
- Then do we need to invent yet another policy header to convey them? (we are with Public-Key-Pins)
  - Also begs question of whether there's need to specify how policies conveyed in HTTP channel are combined and/or conflicts resolved

Further Impetus

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

Requirements for Alternate Policy Conveyance?

- Policy conveyance via same HTTP channel as the protected webapp has first-use MITM vuln
  - see “bootstrap MITM vuln” in HSTS sec cons
- E.g: at least two different folks have suggested leveraging RFC6415 “web host metadata”
  - which leverages RFC5785 “well-known URI”
- There's likely detail-level requirements for overall policy expression, advertisement, conveyance that ought to be thought about at least some.

Underway:

- 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)