draft-ietf-websec-framework-reqs

Jeff “=JeffH” Hodges
IETF-86
Orlando, Florida, US
March 2013

Present Status 1

- A WebSec WG item as of IETF-85 Atlanta: `draft-ietf-websec-framework-reqs-00`
- Attempts to broad-brush sketch overall Web Application problem space
- Leverages (early) Content Security Policy discussion from public-web-security@w3.org list
- Still fairly rough, though made progress on re-organization (source discussions relocated to appendicies)

Present Status 2

- Some additional requirements sources being leveraged:

  Joel Weinberger. *Analysis and Enforcement of Web Application Security Policies*, Doctoral thesis, Dec-2012.

  X Li, Y Xue. *A Survey on Web Application Security*, Technical report, Vanderbilt University, 2011.

  Others?

Plans

- -01 is in progress
- Continue refinement of prose
- Fold in material from new sources
- 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)
- Engage in on-list discussion with reviewers :)

That's all for now, unless we wish to review slides presented at IETF-85 Atlanta (included below)

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 doing so 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.