draft-ietf-websec-strict-transport-sec

Jeff “=JeffH” Hodges

IETF-81

Quebec City, Canada

Overall Status

- draft-ietf-websec-strict-transport-sec-01 submitted on 14-Mar-2011
- -02 in progress (I have local working copy)
- Goal to submit -02 this week or next
- Present spec implemented in Firefox and Chrome
  - more coming?
- 80+ web apps issue STS policy
  - per www.shodanhq.com
- Get to WG Last Call ?

Detailed Status

- All formally open issues are detail-level spec clarifications
  - “formally” == tracker ticket exists
- 12 open tickets
  - 3 tickets are closely related
    - so actually 10 *distinct issues*
  - still combing through list threads to note such issues

Tickets #2, 3, 12: HTTPbis Dependency & Effective Request URI

- #2: Effective Request URI definition dependency on HTTPbis spec ?
- #3: Better Effective Request URI definition ?
- #12: Remove dependencies on HTTPbis and depend on RFC2616 only
  - e.g. in ABNF defining `Strict-Transport-Security` header field

Tickets #2, 3, 12: HTTPbis Dependency & Effective Request URI (cont'd)

- Done in -02 working copy:
  - #2: Effective Request URI definition dependency on HTTPbis spec ?
    - Decided: do not depend on HTTPbis, define in HSTS spec
  - #3: Better Effective Request URI (ERU) definition
    - Done
    - Copied ERU definition from `draft-ietf-httpbis-p1-messaging-15`
  - #12: Remove dependencies on HTTPbis and depend on RFC2616 only
    - Done
    - e.g. in ABNF defining `Strict-Transport-Security` header field

Other Tickets: Detail-level clarifications

- #1: port mapping should be explicit about case where URI does not contain explicit port
- #4: Clarify that HSTS policy applies to entire host (all ports)
- #5: Clarify need for IncludeSubDomains
- #6: cite FireSheep as real-life threat HSTS addresses
- #7: clarify and add examples/justification wrt connection termination due to tls warnings/errors

Other Tickets: Detail-level clarifications (cont'd)

- #8: clarify/explain behavior when STS header not returned by known HSTS Host
- #9: explicitly note revocation check failures as errors causing connection termination?
- #10: note that end-entity certs can be dristrib'd to http clients ?
- #11: failing insecure connections and user recourse

Other Items

- Additional HSTS directives ideas are still outstanding
  - LockCert, LockCA, LockEV, etc.
  - See my slides from IETF-81 Prague
    (pertinent ones included at end of these slides in Appendix)
- I/we haven't actively pursued discussing them
  - DANE work addressing them?

Other Items (cont'd)

- However, 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
  - Firefox folk have verbally concurred

Other Items (cont'd)

- Re-raises questions of LockFoo policies in context of
  - HSTS in particular, HTTP channel generally
  - An aspect of next preso (on `draft-hodges-websec-framework-reqs-00`)

To Do

- Near-term ToDo's:
  - Put issues in the Tracker – largely done
  - Update spec per remaining tracker tickets
    - Essentially remaining tickets are all clarifications
- Further-term steps:
  - Go to WG Last Call ?
    - With present spec (no LockFoo directives) e.g. -02
    - Or first resolve LockFoo deliberations specific to HSTS?
    - Note: STS header field ABNF is extensible – can simply "update" STS spec with new directive specs
  - See next presentation

Appendix

- Following slides from IETF-81 HSTS status presentation, included here for convenient reference

(still) Open Issues cont'd

- Gerv suggested (a while back) a “LockCA” notion
  - i.e. cert and/or CA “pinning” (ie “LockCert”)
  - Several people have brought

LockCA

- Add directive to Strict-Transport-Security header field of “LockCA”
- Semantics are that UA remembers not only that site is secure-only, but also that its certs are issued by CA
  - From initial caching of HSTS info?
  - Supplied along with LockCA directive in header field?

LockCert

- Add directive to Strict-Transport-Security header field of “LockCert”
- Semantics are that UA remembers not only that site is secure-only, but also that this is its cert
  - Ie cache cert “fingerprint”
  - From initial caching of HSTS info?
  - Supplied along with LockCert directive in header field?

EVOnly

- Similar but different from LockCA
- There's operational issues with LockCA
  - Eg what if site wishes to change their CA?
- With EVOnly, UA notes that site's cert MUST be an EV cert.
  - Leverages EV infrastructure (CA/Browser Forum)
  - Site can change CA
- Issues
  - some IETF folks don't recognize CABF Guidelines as referenceable spec
  - Need IANA registry for EV CPS OIDs ?