Resolving Issues in HPKP

Chris Palmer <palmer@google.com>
Ryan Sleevi <sleevi@google.com>

Progress

Went through WGLC.

Published -08.

-09 coming soon; could be last one.

Is the SPKI the right thing to pin?

Vs. trust anchor set names like "symantec".

The proposals are complementary; can do both.

Hard to manage the sets' names and their likely-volatile memberships.

Hard to know what SPKIs to pin to. (Hence report-only mode).

Is the SPKI the right thing to pin?

Proposed resolution: Mention the possibility for trust anchor set names in the future, mention trade-offs, and stick with SPKIs.

Interaction with pre-loaded pins

Current text represents WG consensus.

Proposed resolution: No change.

Interaction of pin scope with cookie scope

Attack: cookie has scope *.example.com; pin domain is example.com with includeSubDomains *not* set. evil.example.com, unpinned, can get cookies. (In many UAs, evil.e.c would still need a valid certificate.)

Proposed resolution: In Security Considerations, recommend that sites using broadly-scoped cookies also pin to the same broad scope.

Well-known URI vs. response header

Bandwidth cost of header is marginal, but people perceive it to be high. Using a W-K- URI would save that, but the savings would be similarly marginal.

W-K URI introduces a blocking load in the path for loading pages/resources, increased page-load latency.

But, it's cacheable.

Well-known URI vs. response header

Proposed resolution: Mention the possibility of a W-K URI arising in the future, discuss why it's not done now: we would want to combine HSTS, HPKP, and CSP into a W-K URI proposal. That is a bigger job; hence defer for now.

Question: Should that text require or suggest UAs to let the W-K URI take precedence over response headers?