WebSec

Berlin, July 2013

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Agenda

- Agenda Bashing + Blue Sheets
- Document Status
- HPKP wrap-up
- Session Continuation
- Open Mic

Document Status

- X-Frame-Options is ~~on its way to~~ ***in*** IETF LC.
- Framework-Reqs – no new version. ~~No~~ Hardly any mailing list discussion.
- HPKP has gone through a WGLC
  - Several issues raised
  - Will be discussed here
- Nico has submitted a revised session continuation problem statement
  - Do we have the energy and people to do this?

HPKP STATUS

SESSION CONTINUATION

Session Continuation

- Suggested at the HTTP-Auth BoF in Atlanta.
- Discussed at WebSec in Orlando.
- Lots of enthusiasm for this to get done.
  - Not as much volunteering to review
- Issue keeps coming up in many places, especially the httpbis ML.
- Following presentation from Nico & Yaron shows what the draft is about.
- Note that previous attempt at httpstate didn't get off the ground.

SESSION CONTINUATION PROBLEM STATEMENT PRESSO

Session Continuation - Solutions

- Origin Cookies
  - Cookies that are only sent to the origin server
  - Bortz/Barth/Czeskis
- Channel ID
  - draft-balfanz-tls-channelid
  - Adds a public key to the TLS handshake
  - Allows for channel-bound cookies
- Session continuation protocol
  - Nico Williams and others.

Session Continuation - Solutions

- HTTP Session Management
  - Phillip Hallam-Baker
- CAKE
  - Adam Barth (expired draft)
- Smart Cookies
  - Trevor Perrin's in a ML message on 22-Jul

- Probably some more that I missed

Session Continuation

- Do we have people to review the problem statement?
- Do we have people who will consider several proposals and pick one as a starting point?
- Do we have people who will carefully read and review a WG solution document in this area?
- Do we have the necessary expertise in the room or on the mailing list?

OPEN MIC

SESSION CONT PROBLEM SLIDES (IN CASE WE DON'T GET IT FROM NICO)

Session Continuation – Problems

- Bearer Token
  - Cookies are transmitted frequently, and if a transmitted cookie is somehow stolen, it could be used by an attacker.
- Cookie Scope
  - Cookies are sent to (malicious or compromised) subdomains.
    - "Domain" attribute fixes this, but not on all browsers
  - Such subdomains can modify or erase cookies.

Session Continuation - Problems

- Cookie Availability
  - Cookies can be used by any page or script running in the browser.
  - HTML and script from any site can use the user's cookies to "bless" their requests.
  - This enables CSRF (although we know how to mitigate that, and also a privacy issue, as it helps sites track users).
- Missing an explicit "logout" available to either side.
- Cookie behavior cannot be changed.