WebSec Minutes

WebSec met on Wednesday, March 13, at 17:10, for 1.5 hours. Thanks to Brad Hill for taking minutes. We had three items on our agenda:

Framework Requirements

Jeff Hodges, who is also editing the draft presented. The document draft-ietf-websec-framework-reqs is a new WG document submitted just last month. Still very rough, and includes references to only two scholarly articles. More would be appreciated. Jeff is working on version -01 which will polish the text further.

There was no discussion, and only 2 people other than Jeff have read the draft.

Key Pinning

Ryan Sleevi presented. The document currently has 5 open issues, and we discussed them all:

- Issue #52 – clarification that max_age parameter is required, and that max_age of zero means removal of the pin. People agreed that draft -04 solves the issue, so it is now closed. EKR noted that the draft should specify a maximum max_age of maybe 30 days or 3,000,000 seconds (34.7 days). JeffH asked why this was necessary for PKP but not for STS, and EKR said this was because sites were not likely to switch back from secured to non-secured, but likely to brick themselves if they ever want to change certificate vendor, or if the vendor changes keys. We may need a new issue for this.
- Issue #53 – dealing with private trust anchors. The text in -04 has added a **`strict`** parameter, which instructs the UA to always enforce the pins. Without this, the UA MAY choose not to block in the face of certificates signed with private (rather than stock) trust anchors. Paul Hoffman said that the intent of **`strict`** was not sufficiently clear. Consensus is that the **`strict`** directive solves the issue, but the processing should be clarified before issue #53 can be closed.
- Issue #54 – Report Only. draft -04 contains a header that will cause the browser to not enforce pins, but rather, it will just report when pins are violated. This is used to test policies before asking UAs to enforce them. It is not a security feature. EKR said this answers his requirement. This issue can now be closed, unless discussion on the list reveals some privacy issue with sending these reports.
- Issue #55 – Interaction with pre-loaded pin list. Version -04 of the draft clarifies that the latest observed pin is the determining one. This implies that list of pre-loaded pins (pushed during installation of software update) should contain timestamp of observation. We can probably leave

it at that, mention the timestamp issue in implementation advice, and close the issue.

- Issue #56 – includeSubDomains – this was added. It means that the policy specified in the header affects subdomains as well. As with HSTS, superdomain policy should win. JeffH agrees that more text and operational consideration is needed. Also need clarification that PKPs for EE certificates would not work with includeSubDomains.

A few more issues were raised:

1. There is a requirement for backup pins. This is especially hard with EE PKPs, so most would back up with a CA pin.
2. Interesting interaction with other types of pinning like TACK. EKR says we should ignore it, and anyway TACK is not progressing.
3. Section 2.8 talks about self-signed (or self-issued) certificates. Should mention DANE type #3, because those are as "rooted" as CA certificates.

Session Management

The chair talked about how the issue came up, about the design team that was convened to create the draft and about the problem that needs solving. PHB presented the problem statement draft.

Draft: http://tools.ietf.org/html/draft-williams-websec-session-continue-prob

Presso: http://www.ietf.org/proceedings/86/slides/slides-86-websec-3.pdf

During Phil's presentation there was some discussion on the per-request authentication and mechanisms to achieve it, and a few other issues.

After that we went back to the chair's slides, and we polled the room to see if this could become a working group item.

Several people (including Paul H, Jeff H, Y Oiwa, and several others) said that this is a good and important thing for the IETF to work on. When asked who thought otherwise, nobody spoke up.

When asked whether this WG is a good fit for this topic, Jeff H, Nico and several others said yes, Paul H suggested that HTTPAuth might be more appropriate because the security people are there, or at HTTPbis because the browser people are there. Yoav (speaking as HTTPAuth chair) said that HTTPAuth's charter is too narrow. HTTPbis declined to adopt previous attempt at the same topic. There was consensus to at least start it at WebSec, although it may later move[*].

When asked, about 6 people promised to review the draft before when we call for adoption, and there was weak support to choose this draft over trying to write a different draft. We will take this to the list, and begin to work on this.

This ended the WebSec meeting.

([*]) After the session, I talked with Barry (our AD), and we can begin work on this as if it's a charter item. When it becomes necessary, we will discuss re-chartering, but we can begin even before that.