

Implementation Challenges with Browser Security

IAB Technical Plenary,
March 2012, Paris

Moderator: Hannes Tschofenig

Background and Motivation

- You may have noticed the increasing number of data breaches and security incidents.
- Many reasons for these problems:
 - misconfiguration, questionable operational practices, implementation bugs, etc.
 - Most aspects outside the scope of the IETF.
- To keep up with the changing threat landscape we have a long history in developing security protocols forming the foundation of today's communication systems.
- Internet security is a large topic and therefore we have to focus our discussion today on the Web.

"The Web" (aka "the open web platform") is ...

- the interlinked world you experience via your web browser(s) and/or mobile device(s) and their applications.
- a constantly and rapidly evolving ecosystem ...
 - based on extensible dynamically-configurable foundation: DNS, TLS, HTTP, URIs, HTML, XML/JSON, JavaScript, etc.
 - with few barriers to experiment openly in the wild
 - Using self-modifying mobile code with browsers/devices are execution environments, but lack many of the protections that OSs have evolved.
- the basis for galaxies of non-trivial interlinked web application ecosystems delivering real value.

See IAB technical plenary on "Post Standardization" (Prague IETF meeting, March 2011):

<http://www.ietf.org/proceedings/80/technical-plenary.html> and <http://tools.ietf.org/html/draft-tschofenig-post-standardization>

Unfortunately, new exploits for the previously mentioned technologies emerge almost daily.

Key Questions

- How do we evolve the security characteristics of the web platform such that ...
 - new web platform components can be slid "underneath" existing web apps while minimizing disruption
 - existing web apps can be smoothly enhanced to take advantage of new secure web platform features
 - entirely new web apps with better-than-present security characteristics are enabled
- Experience has shown the transition phase creates problems.

Plenary Agenda

- Panel members share their experience:
 - Eric Rescorla (RTFM)
 - Thomas Lowenthal (Mozilla)
 - Chris Weber (Casaba Security)
 - Ian Fette (Google)
 - Jeff Hodges (PayPal)
- Questions and feedback from the audience.