Web User Empowerment Concept

Andrew Fregly, Verisign Inc
Verisign W3C AC Representative

Overview

Web user empowerment is proposed as an approach to give Internet users control over their privacy and security on the Internet. The concept addresses an issue that many people have with the Web, which is that they are at the mercy of websites when it comes to the mechanisms for authentication and disclosure of personal information. Web user empowerment flips the paradigm for authentication and exchange of personal information by allowing users to declare how secure they want authentication to be (i.e. always use true two-factor authentication for financial transactions) and also to declare rules for how they want personal information to be made available (i.e. allow non-friends on social networking sites to see only my first name and the country I live in). The concept defines the mechanism by which users can do this and also how websites/web applications would be able to conform with user declarations (policies).

There is some history of this type of capability being explored or pursued. What is different about this concept is that policy management and services implementing policy are to be provided by standards-based browser APIs that are accessed through HTML5 enhancements and JavaScript. This makes the browser the control point for policy access, policy management, and code that implements policy. This is a huge improvement versus current mechanisms that rely on policy definition and enforcement implemented by application code running on websites. The idea may also be extended to define service layers within IOS, Android and other operating systems so as to provide the same capabilities to apps on these devices.

Challenges

- Determining where to store private information and how it can be securely managed.
- This introduces a new paradigm for web apps interacting with the browser.
- The implementing the technology in a way that fulfills the intent
- Adoption will be a big challenge

Risks

- It will be a challenge to get this approach adopted by service providers and websites. A lot of effort could be put into specifying the capability and then it would not get adopted.
- Poor implementations could introduce security and privacy risks exceeding those that the approach is trying to solve.

Note: The author of this submission became aware of this opportunity on the last day to file a submission. Due to consequent urgency to get something out, research into prior consideration or work in this area has not been done. The time constraint has affected the comprehensiveness of the submission. The author also does not know at the time of filing whether or not he will be given approval by his organization to present the concept at the workshop.