NSTIC, Privacy and Social Login

Presentation at the W3C Workshop on Identity in the Browser

Francisco Corella and Karen P. Lewison

Pomcor
Getting Rid of Passwords...

- ...is one long term goal of NSTIC
- But it may be achieved in the short term by “social login”
  - Login with Facebook...
  - ...or some other social site such as MySpace or LinkedIn or Twitter
  - ... or a general purpose site such as Google or Yahoo
- Is this a good thing?
Unfortunately Not!

- NSTIC seeks increased privacy and security, OAuth-based social login achieves the opposite:
  - Social site can track user’s Web activity
  - Credential may be sent in the clear
  - Facilitates phishing attacks
- RPs must register with social site
  - Social site can revoke registration
- Registration requirement reinforces Facebook’s social network monopoly
Social Login Needed ASAP in the NSTIC Ecosystem

- In the long term, the NSTIC ecosystem should be based on ZKP technology.
- But today’s social login may preempt NSTIC if we wait until ZKP can be broadly deployed by RPs.
- => NSTIC needs an interim solution.
- The interim solution could be used to develop a trust framework and user interfaces ahead of the long term solution.
HTTP Extension for Delegated Identity

- Browser aware of double redirection
- Browser retains callback URL
- Browser generates one-time key pair, IdP binds one-time public key to attributes in one-time certificate
- Browser receives generic identifier from IdP, sends RP-specific identifier to RP
  - Generic identifier is high-entropy secret, not included in one-time certificate
Social Login Using the HTTP Extension

- IdP = social site
- RP generates 2\textsuperscript{nd} one-time key pair, sends public key to social site via 1\textsuperscript{st} redirection
- Social site binds 2\textsuperscript{nd} one-time public key to right to access user’s account, in 2\textsuperscript{nd} one-time certificate; sends certificate to RP via 2\textsuperscript{nd} redirection
- RP accesses user’s account at social site using 2\textsuperscript{nd} one-time certificate
For More Info

- A newly revised version of the position paper will be posted to the Pomcor site shortly after the workshop:
- Email addresses of the authors:
  - fcorella@pomcor.com
  - kplewison@pomcor.com