Browsers and Identity Protocols

IETF OAuth WG – ad hoc

November the 2nd, 2020

George Fletcher

Vittorio Bertocci

Agenda

- Anti-tracking, IsLoggedIn & WebID initiatives
- Impact on the OAuth WG work
- Proposal for a WG position on these initiatives
- Discussion

TL;DR

1. As privacy-preserving measure, browser vendors want to restrict primitives essential to today’s protocols
2. To preserve identity protocol functionality, browsers are working on dedicated identity API
3. Once they’re satisfied with 2, they’ll execute on 1 and break today’s protocol

CHALLENGE: the scenarios addressed by 2 are a strict subset of the scenarios the identity community implements.
If 2 isn’t extended appropriately, 3 will result in significant loss

Restrictions – Current and Upcoming

- SameSite – change default cookie scope
  - https://web.dev/samesite-cookies-explained/
- Intelligent Tracking Protection
  - https://webkit.org/blog/category/privacy/
- Bounce Tracking Protection
  - Part of ITP – track sites that use redirects with link decoration
- 3rd party cookies
  - Disabled in Safari, easily disabled in Firefox, going away in Chrome in 2022
- All cookies?
  - Safari already introducing restrictions on 1st party cookies if the domain is classified as a tracking domain

WebID

https://github.com/WICG/WebID

- In a nutshell
  - Preserve Identity Federation
  - While preventing
    - Ad based targeted tracking (bounce tracking)
    - RP collusion
    - IDP privacy leakage (which RPs the user is accessing in an authenticated state)
- Scenarios
  - Primarily focused on personal use of browsers by users
- Issues
  - Academic, First Party SSO, Small Business, Enterprise, …

IsLoggedIn

https://github.com/privacycg/is-logged-in

- In a nutshell
  - Simple state of logged-in/logged-out per domain
  - Use state to manage access to local storage
  - Clear local storage and cookies on logout
  - Only browser mediated authentications are “trusted” (e.g. webauthn or password manager)
- Scenarios
  - Show users where they are logged in
  - Prompt users that they are still logged in to domains they haven’t visited recently
- Issues
  - How does the IDP maintain trust for a given user:browser pair after logout if all cookies are cleared
  - Significantly limits other authentication mechanisms that are convenient for the user (e.g. QR code or push)

Things we could do as WG

- Participate in the working groups/MLs where the new API are being discussed
    - In larger number and/or
    - Giving mandate to WG representatives
- Be more explicit about today’s scenarios and features we want to preserve
    - Put together a doc/spec enumerating scenarios and features
    - Have WGs and vendors weigh in/endorse
    - Refer to the doc in discussions with the browser vendors

Discussion