OAuth 2.0 for Browser-Based Apps

draft-ietf-oauth-browser-based-apps-06

Aaron Parecki

Virtual Interim Meeting
April 6, 2020

OAuth 2.0 for Browser Based Apps

- Includes recommendations for implementors building browser-based apps using OAuth 2.0

- "Browser-based apps" are defined as applications executing in a browser, aka "SPA" or "single-page apps"

OAuth 2.0 for Browser Based Apps

- **MUST** use the OAuth 2.0 authorization code flow with the PKCE extension (no Implicit flow)
- **MUST** protect against CSRF attacks by either
  - ensuring the AS supports PKCE
  - using the OAuth 2.0 state parameter
  - using the OpenID Connect nonce parameter
- The AS **MUST** require redirect URI registration and require an exact match of the redirect URI
- The AS **MUST** rotate refresh tokens, and set a maximum lifetime or idle timeout

What's New Since IETF106?

- Incorporated editorial and most substantive feedback from Mike Jones
- Disallow the password grant even for first-party applications
- Allow refresh tokens in SPAs as long as they conform to Security BCP
- Editorial clarifications

Open Questions

Security BCP Update

- The Security BCP was updated to relax the requirement of PKCE, no longer required, only RECOMMENDED
- Should we update the guidance for browser-based apps as well?
- This is predicated on some rather complex conditions, better left detailed by the Security BCP and referenced here?

Open Questions

Open questions in email thread from Mike Jones

- Adding references to OpenID Connect as an alternative to PKCE? Which response types/modes specifically?

- However any form of issuing access tokens in the authorization response still does not address the problem in 9.6.3 giving the AS assurance that the token was received by the right application

Open Questions

Topics for working group discussion requested by Mike Jones

- Requesting guidance on how to vary application redirect URIs using the "state" parameter safely (avoiding storing things in cookies)

- Can an OpenID Connect signed `request_uri` be used as an alternative to exact redirect URI matching by browser-based apps?

- Offline access refresh tokens are a risk for browser-based apps. Can we provide any recommendations here? e.g. recommending revoking refresh tokens when the user signs out at the AS? (aka `online_access` refresh tokens)

New Items

Service Worker Proxy

Demo Application: https://gitlab.com/jimdigriz/oauth2-worker

- A Service Worker can be used to perform the OAuth flow, get and store access & refresh tokens, and make API requests, all without exposing the tokens to code on the page

- Add this as an architectural pattern to the list?