OAuth 2.0 Step-up Authentication Challenge Protocol

Backstory/Context/Problem Statement

• Protected resources can reject *technically valid* access tokens for any reason
  • Opaque risk engine decisions, local constraints (e.g., high risk transactions), bad vibes, etc.

• Often what the RS wants is:
  • A token obtained from a more recent authentication event, or
  • A token obtained with a different authentication flow

• There’s currently no standardized guidance on how:
  • The RS can express its requirements to the client
  • The client can indicate those requirements to the authorization server
Summary of Draft’s Approach

- Extend RFC6750 challenge with
  - error code insufficient_user_authentication
  - New WWW-Authenticate params acr_values & max_age

- Utilize authorization request parameters acr_values & max_age (already in the OAuth Parameters registry via OIDC core)

- Define/reference acr & auth_time Introspection response parameters and JWT claims to express information about the authentication event associated with the access token to the protected resource
(1) GET /api/highvalue HTTP/1.1
Host: example.com
Authorization: Bearer chX9Kl_26jiQVvACD77Epc5T

(2) HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer error="insufficient_user_authentication",
  error_description="more recent user authentication is needed", max_age="5"

(3) GET /as/authorization.oauth2?client_id=xHMM&response_type=code&scope=purchase&max_age=5

(4) HTTP/1.1 200 OK
{
  "access_token": "16Kx687pSoL9wvd4fn2eu21",
  "token_type": "Bearer"
}

(5) GET /api/highvalue HTTP/1.1
Host: example.com
Authorization: Bearer 16Kx687pSoL9wvd4fn2eu21

(6) HTTP/1.1 200 OK ...
...

[... the magic happens ...]

browser

protected resource

authorization server

client
We’ll always have Vienna

- First presented at IETF 113
- WG Adoption not long after followed by typical iterations (-01 / -02)
Happenings since IETF 114 Philly

- 03 (Sept 14)
  - Clarified that acr_values and max_age can co-occur in the challenge, when/if necessary
  - Fleshed out deployment and security considerations and also IANA stuff
  - Attempt to clarify that while acr_values can have more than one value, only one of them is used and ends up in the token

- Moved repo to the oauth-wg github org (Sept 15)

- WGLC (Sept 22 – Oct 7)
- 04/05 (Oct 10/11)
  - Editorial updates/notes from WGLC feedback
  - Updates to the updates

- Update examples/figures to be clear that the authorization request is sent by the client via directing the user agent (editor’s draft with -06 coming soon)

- Shepherd Review (anticipated soonish)
Looking ahead... IETF 116 Prague

• Hopefully this will be the last time seeing a presentation on this
• I’m not going to be able to make it to Prague anyway