OAuth 2.0 Security Best Current Practice

draft-ietf-oauth-security-topics-19

T. Lodderstedt
J. Bradley
A. Labunets
D. Fett

Current Status

To be edited in:

- Rifaat’s feedback from Shepherd's Writeup
- Mike Jones’ feedback

Feedback:

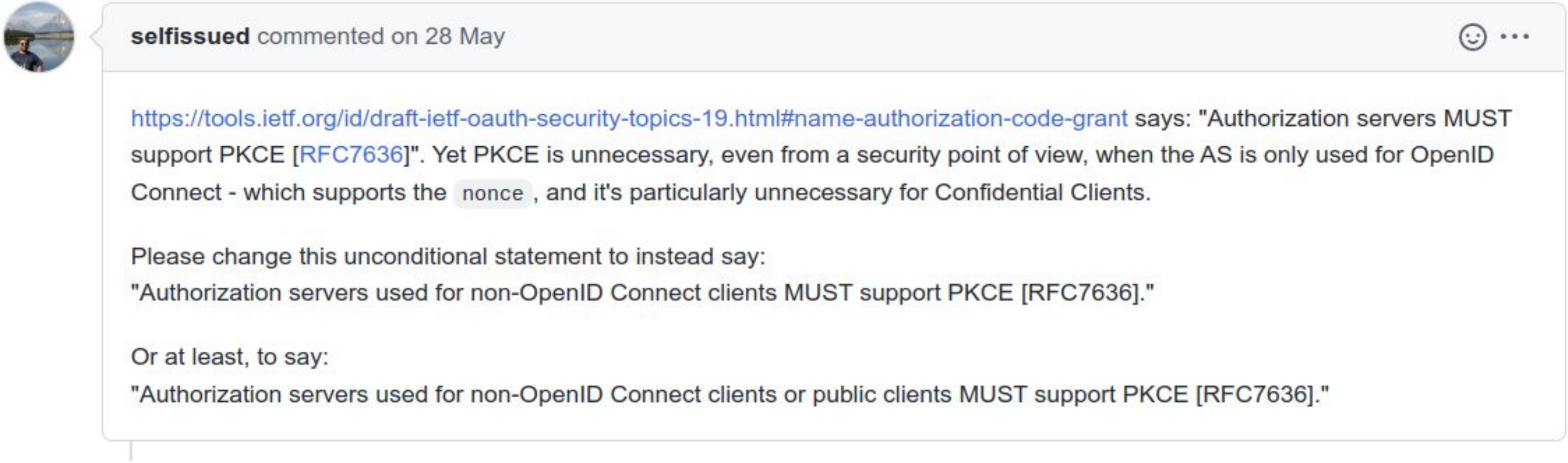
- Various editorial stuff
- Update to references
- Lack of clarity in explanations of attacks and mitigations
- Missing references to other specs (e.g., JWT access token profile, DPoP)
- PKCE-support mandatory for ASs?

What happened in Vienna stayed in Vienna

Summary of IETF 113 discussions:

- Rules around PKCE are fine
  - Obligations for clients to use PKCE, not for servers to enforce PKCE
- Need more explanation!

PKCE (again?!)



selfissued commented on 28 May

https://tools.ietf.org/id/draft-ietf-oauth-security-topics-19.html#name-authorization-code-grant says: "Authorization servers MUST support PKCE [RFC7636]". Yet PKCE is unnecessary, even from a security point of view, when the AS is only used for OpenID Connect - which supports the `nonce`, and it's particularly unnecessary for Confidential Clients.

Please change this unconditional statement to instead say:
"Authorization servers used for non-OpenID Connect clients MUST support PKCE [RFC7636]."

Or at least, to say:
"Authorization servers used for non-OpenID Connect clients or public clients MUST support PKCE [RFC7636]."

Every AS should offer PKCE!

PKCE provides a robust defense against CSRF
(see IETF113, now also explained in draft)

More robust than nonce:

- Authorization response may contain nonce → attacker can intercept and replace with new authorization response matching nonce
- Check is AS-enforced, cannot be skipped by client

MAY CONTAIN TRACES OF NONCES

Every AS should offer PKCE!

More important: Consistency for clients!

With consistent PKCE support, clients and whole ecosystems can move from state to PKCE.

Proposal: Keep as-is

- Clients:
  - Public clients MUST use PKCE
  - Other clients SHOULD use PKCE (nonce as alternative, under precautions)
- AS:
  - MUST support PKCE
  - No requirement to enforce PKCE

Next Steps

- Finishing up -20 (this week?)
- Closing all issues in https://github.com/oauthstuff/draft-ietf-oauth-security-topics/issues
- Continue finalizing process