OAuth 2.0 Security Best Current Practice

draft-ietf-oauth-security-topics

IETF-106, 20.11.2019, Singapore

Daniel Fett, John Bradley, Andrey Labunets, Torsten Lodderstedt

Status

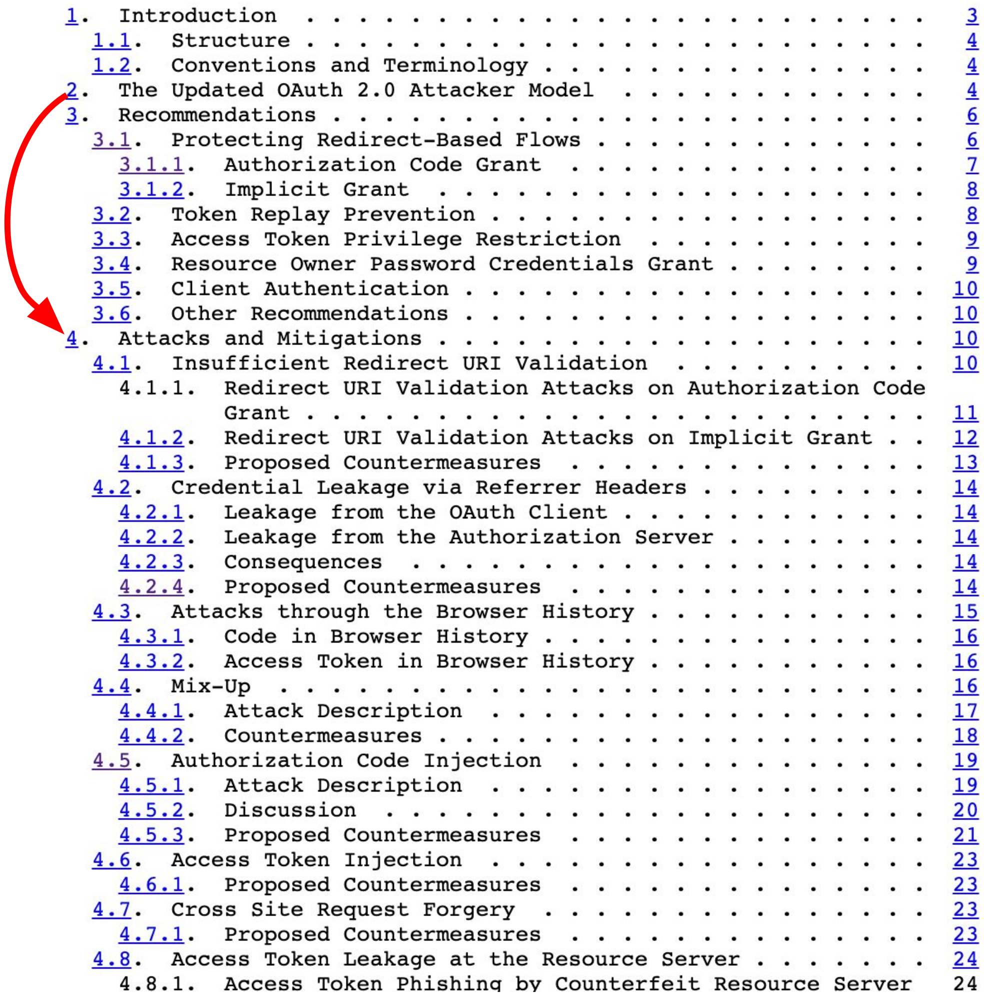
- Decided to move draft forward to publication and to start work on solution for “PKCE Chosen Challenge Attack” in subsequent version of the BCP (Call 04.11.2019)
- Draft is in WGLC since 06.11.2019
- Received some review feedback
- Mostly editorial and requests for clarifications
- "Alice and Bob Collusion" was brought up again
- Open issue on later slide

Communities using the OAuth Security BCP

- Financial-grade API (FAPI) working group (OpenID Foundation)
  - Alignment towards BCP ongoing
  - Provides profiles for security sensitive applications with stronger requirements on top of BCP
- NextGenPSD2 (aka Berlin Group)
  - Refers to BCP in recently released security bulletin
  - Service providers in Rumania (namely IT Smart Systems) recommend Security BCP to banks
  - PBZ (Privredna banka Zagreb d.d.) in Croatia uses Security BCP
- HelseID (eHealth) in Norway uses Security BCP
- Cloud Signature Consortium (CSC) refers to Security BCP
- JS libraries (e.g. angular-oauth2-oidc) now support code+PKCE and vendors start to adapt their documentation (e.g. Identity Server)

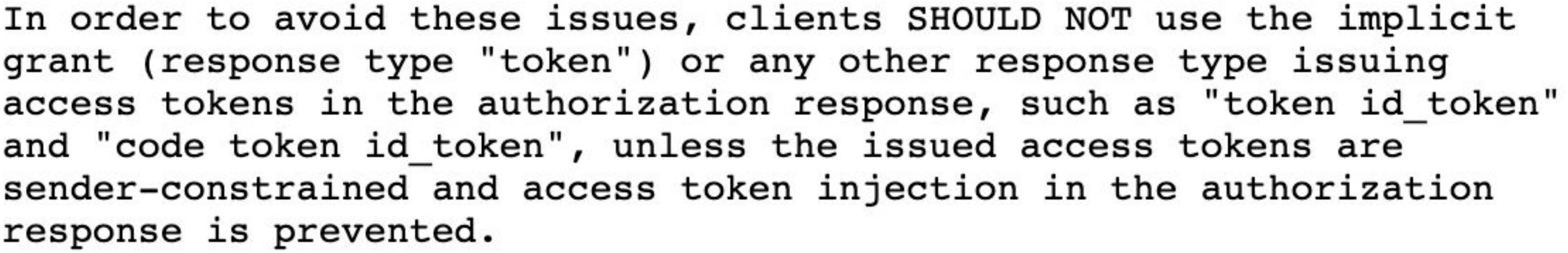
Next Steps

- Rework Introduction to clearly state relationships to RFC 6749, 6750 & 6819 and clean up language
- Move Attacker Model (Section 2) after Recommendations (Section 3) - easier to read for people only interested in following the recommendations
- Make PKCE mandatory for AS



Open

- Hans Zandbelt raised the question re SHOULD NOT or MUST NOT for implicit again (and Rob Otto supported it on the list)
- Here is the current text:



In order to avoid these issues, clients SHOULD NOT use the implicit grant (response type "token") or any other response type issuing access tokens in the authorization response, such as "token id_token" and "code token id_token", unless the issued access tokens are sender-constrained and access token injection in the authorization response is prevented.

OAuth Security Workshop 2020

- 22-24 JULY 2020 IN TRONDHEIM, NORWAY
- https://osw2020.com/

#osw2019

#osw2020