draft-ietf-oauth-security-topics

Status

John Bradley, Andrey Labunets, Torsten Lodderstedt

IETF-101
March 19 2018, London

What is it?

- Comprehensive overview on open OAuth security topics
- Systematically captures and discusses these security topics and respective mitigations
- Recommends best current practice and OAuth changes & extensions

Structure

Recommendations

Threat Analysis and Discussion of Counter Measures

Recommendations

- Exact redirect URI matching at AS (token leakage, mix-up)
- Avoid any redirects or forwards, which can be parameterized by URI query parameters (open redirection, token/code leakage)
- One-time use tokens carried in the STATE parameter for XSRF prevention
- AS-specific redirect URIs (mix-up)
- Clients shall use PKCE (or nonce) to prevent code injection
- Use of TLS-based methods for sender constraint access tokens
- Use end-to-end TLS whenever possible

Status

- Published revisions -05
- Completed sections on code leakage via referrer header, attacks in browser, mix-up, and CSRF
- Reworked Code Injection Section
- removed refresh token leakage as respective considerations can be found in section 10.4 of RFC 6749
- Added open redirection

Ready to become a BCP