draft-ietf-oauth-security-topics
Status

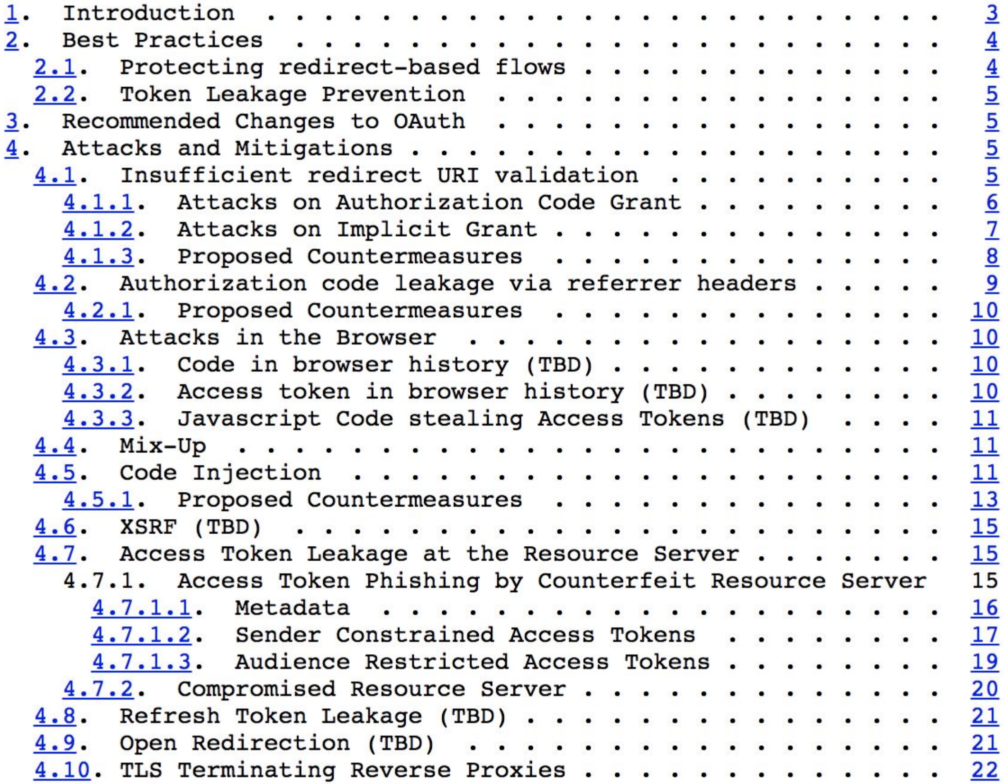
John Bradley, Andrey Labunets, Torsten Lodderstedt

IETF-100
Nov 15 2017, Singapore

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

Recommended Best Practices

- 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 in order to detect code injection
- Authorization servers shall use TLS-based methods for sender constraint access tokens
- Use end-to-end TLS whenever possible

Recommended Changes to OAuth

Remove requirement to check actual redirect URI at token endpoint (RFC 6749, Section 4.3.1)

“ensure that the "redirect_uri" parameter is present if the "redirect_uri" parameter was included in the initial authorization request … and if included ensure that their values are identical.”

- Objective: prevent client impersonation/code injection
- Challenges:
    - seems to complicated to implement properly and requires transaction specific state
    - Some implementations short cut be just pattern matching against client policy
- protection goal is achieved more effective by utilizing PKCE as recommended

Status

- Published revisions -03 & -04
- Added text on token leakage at the resource server based on discussions in Prague
  - Additional Metadata
  - Audience Restriction
  - Sender Constraint Access Tokens
- Added text on threats associated with use of TLS Terminating Reverse Proxies
- Based on feedback in Prague, added recommendation to use sender constraint access tokens as prefered countermeasure against token leakage
- Restructured BCP

Please give us feedback!