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

1. Introduction .................................................. 2
2. Recommendations .............................................. 4
   2.1. Protecting redirect-based flows ....................... 4
   2.2. Token Replay Prevention ............................... 5
3. Attacks and Mitigations ....................................... 5
   3.1. Insufficient redirect URI validation ................... 5
       3.1.1. Attacks on Authorization Code Grant .......... 5
       3.1.2. Attacks on Implicit Grant ....................... 6
       3.1.3. Proposed Countermeasures ....................... 8
   3.2. Authorization code leakage via referrer headers .... 9
       3.2.1. Proposed Countermeasures ....................... 9
   3.3. Attacks in the Browser .................................. 10
       3.3.1. Code in browser history ......................... 10
       3.3.2. Access token in browser history ............... 10
   3.4. Mix-Up ................................................ 11
   3.5. Code Injection .......................................... 11
       3.5.1. Proposed Countermeasures ....................... 13
   3.6. Cross Site Request Forgery ............................. 15
   3.7. Access Token Leakage at the Resource Server ....... 15
       3.7.1. Access Token Phishing by Counterfeit Resource Server 15
           3.7.1.1. Metadata ..................................... 16
           3.7.1.2. Sender Constrained Access Tokens .......... 17
           3.7.1.3. Audience Restricted Access Tokens .......... 19
       3.7.2. Compromised Resource Server .................... 20
   3.8. Open Redirect .......................................... 21
       3.8.1. Authorization Server as Open Redirector ....... 21
       3.8.2. Clients as Open Redirector ........................ 21
   3.9. TLS Terminating Reverse Proxies ...................... 22
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