OAuth 2.0 Security Best Current Practice

draft-ietf-oauth-security-topics

Status

John Bradley, Andrey Labunets,
Daniel Fett, Torsten Lodderstedt

IETF-102
July 19 2018, Montreal

What is it?

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

Structure

Recommendations

Threat Analysis and Discussion of potential 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

- Some review feedback during/after IETF-101 (-05)
- Incorporated feedback into latest revision (-06)
  - Reworked text on open redirection (esp. redirect behavior of AS in case of erroneous requests)
  - Reworked section on mix up (thanks to our new co-author Daniel Fett)
  - replaced text intended to inform WG discussion by recommendations to implementors (turned draft into BCP)
- No further (reasonable) feedback
- Two open proposals, otherwise ready to proceed

Adopt proposals? WG Feedback needed!

- Audience restriction - Johan Peeters proposed an additional section on the value of audience/action restricted access tokens

https://www.ietf.org/mail-archive/web/oauth/current/msg18117.html

- Crypto Agility - Doug McDorman proposed an additional section on crypto agility.

https://www.ietf.org/mail-archive/web/oauth/current/msg18118.html