OAuth Security Topics

IETF-98, Chicago

Andrey Labunets, John Bradley, Torsten Lodderstedt

Status

- Adopted and pubished as working group document
  - https://tools.ietf.org/html/draft-ietf-oauth-security-topics-02
- Changed type to BCP

Status (cont‘d)

- First focused on protection of the redirect-based flows
- Proposed Best Practice:
  - Strict redirect URI matching
  - AS-specific redirect URIs
  - One-time use, user agent bound XSRF tokens in STATE
  - One-time use, user agent bound PKCE challenge to detect code injection
- Further proposal
  - Drop check of actual redirect URI at token endpoint

Next Step

- Dynamic OAuth, e.g.
  - Token leakage at bad resource servers
  - Mix Up

Please review and comment!