OAuth Security Topics

IETF-98, Seoul

Andrey Labunets, John Bradley, Torsten Lodderstedt

Motivation

- Practical use of OAuth 2 revealed implementation weaknesses and anti-patterns (e.g. XRSF, redirect URI matching, referrer headers)
- Technology has changed (e.g. fragment handling, claimed URLs)
- OAuth is used in much more complex & dynamic setups than originally anticipated (trust model)
- Security Considerations in RFCs 6749/6750 & Security Threat Model (RFC 6819) no longer suffice

Objective of the Document

- Working document used to
  - Capture open security topics,
  - Document and assess potential mitigations,
  - Document the status of discussion in the WG
- Documention in this document or references to other drafts

Long-Term Goal

- Define OAuth extensions if needed (other documents)
- Aim to provide implementers with specific and clear guidelines how to implement OAuth securely (BCP), e.g.

  1) Do exact redirect_uri matching,

  2) Implement PKCE,

  3) …

Status

- OAuth Credentials Leakage
  - **Redirect URI validation of authorization requests**
    - **exact redirect URI matching**
    - **JWT Secured Authorization Request (JAR)?**
    - **...**
  - **Authorization code leakage via referrer headers**
    - **rel="noreferrer"**
    - **"referrer" meta link**
    - **...**
  - Code in browser history (TBD)
  - Access token in browser history (TBD)
  - Access token on bad resource servers (TBD)
  - Mix-Up (TBD)
- OAuth Credentials Injection
  - **Code Injection**
    - **Nonce, State, PKCE, Token Binding, ...**
  - Access Token Injection (TBD)
  - XSRF (TBD)
- Open Redirectors (TBD)

Way forward

1) Complete threat descriptions and discuss mitigations – Next Topics?

2) Agree on recommended mitigations

3) Start work on OAuth Security BCP