OAuth WG @ IETF#95

Hannes Tschofenig, Derek Atkins

Developments since Yokohama

- **OAuth Security Workshop/December 2015** (per-invitation only workshop hosted by Deutsche Telekom)
- **Mix-Up Security Vulnerability**
  - http://www.ietf.org/mail-archive/web/oauth/current/msg15336.html
- **Mailing List for submitting OAuth security vulnerabilities**
  - http://www.ietf.org/mail-archive/web/oauth/current/msg15347.html
- **Announcement of OAuth Security Workshop/July 2016**
- **Re-chartering / Milestone update**

NEW Milestones

Date	Milestone
Nov 2016	Submit 'OAuth 2.0 for Native Apps' to the IESG draft-ietf-oauth-native-apps
Oct 2016	Submit 'OAuth 2.0 Device Flow' to the IESG draft-ietf-oauth-device-flow
Jul 2016	Submit 'A Method for Signing HTTP Requests for OAuth' to IESG draft-ietf-oauth-signed-http-request
Jul 2016	Submit 'OAuth 2.0 Proof-of-Possession: Authorization Server to Client Key Distribution' to the IESG draft-ietf-oauth-pop-key-distribution
Jul 2016	Submit 'OAuth 2.0 Security: Closing Open Redirectors in OAuth' to the IESG draft-ietf-oauth-closing-redirectors
Jul 2016	Submit 'OAuth 2.0 Token Exchange' to the IESG for consideration as a Proposed Standard draft-ietf-oauth-token-exchange
Jun 2016	Submit 'OAuth 2.0 Mix-Up Mitigation'to the IESG draft-ietf-oauth-mix-up-mitigation
May 2016	Submit 'Authentication Method Reference Values' to the IESG draft-ietf-oauth-amr-values
Apr 2016	Submit 'OAuth 2.0 Authorization Server Discovery Metadata' to the IESG draft-ietf-oauth-discovery
Apr 2016	Submit 'Request by JWS ver.1.0 for OAuth 2.0' to the IESG for consideration as a Proposed Standard draft-ietf-oauth-jwsreq
Done	Submit 'Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)' to the IESG draft-ietf-oauth-proof-of-possession
Done	Submit 'OAuth 2.0 Proof-of-Possession (PoP) Security Architecture' to the IESG draft-ietf-oauth-pop-architecture

OAuth Security Workshop

- July 14th and 15th 2016 in Trier/Germany
- **Position paper submission deadline: May 21, 2016**
- Organizers seek input for OAuth- and OAuth-related security investigations. This includes ACE.

Agenda

OAuth 2.0 Mix-Up Mitigation (45 min)

https://datatracker.ietf.org/doc/draft-ietf-oauth-mix-up-mitigation/

Presentation about the problems/threats we are solving:

(a) OAuth Mix-Up (John)

(b) Cut-and-paste Attack (Nat)

Move cut-and-paste threat to a different document?

Agenda (2)

OAuth Discovery (45min)

- What are the use cases the discovery document is solving?
- OAuth 2.0 Authorization Server Discovery Metadata (Mike, 15 min)
- https://datatracker.ietf.org/doc/draft-ietf-oauth-discovery/
- OAuth Response Metadata (Nat, 15min)
- https://datatracker.ietf.org/doc/draft-sakimura-oauth-meta/
- OAuth 2.0 Bound Configuration Lookup (Phil, 15min)
- https://tools.ietf.org/html/draft-hunt-oauth-bound-config-00

Agenda (3)

Token Exchange (Brian, 15 min)

https://datatracker.ietf.org/doc/draft-ietf-oauth-token-exchange/

What has been done and discuss open issues?

Implementation status? Interoperability?

Agenda (4)

OAuth 2.0 for Native Apps (William, 15 min)

http://datatracker.ietf.org/doc/draft-ietf-oauth-native-apps/

Presentation of availability of code. Moving the document to WGLC as soon as enough people did interop tests.

Agenda (5)

Resource Indicators for OAuth 2.0
(Brian/John, 15 min)

https://datatracker.ietf.org/doc/draft-campbell-oauth-resource-indicators/

New draft – old concept. Where do we got with this?