SESSION I

Scribe: Tony

Chair Update

2 docs in IESG evaluation

Some docs in the RFC editors' queue

OAuth 2.1

Reading all the RCFs is complicated

Proposed Base for OAuth 2.1

Authz Code + PKCE

Client Credentials

Device Grant

Mike: it's all the stuff in the IANA Registry that you should be looking at and not just the RFCs

So there is support for doing something, not sure what it would look like, so follow on discussions need to happen.

What information do we have and what do we need to make this choice?

OAuth 2.0 for Browser-Based Apps

Draft has been going for about a year

Must use authz code flow with PKCE

MUST NOT return access tokens in front channel

Disallow the password grant

Allow refresh tokens in SPA

Editorial clarifications

Should "state" be used fort CSRF protection even if PKCE is used

PKCE should be enough, Security BCP makes PKCE mandatory

Making STATE mandatory would brake core spec since it's optional param

So the BBA BCP should point to the Security BCP and not add any text here

Open Issues

Refresh tokens, should the BCP make suggestions on how to silently refresh tokens in a browser?

Not make any decisions in this BCP for Refresh Tokens

Content Security Policy

Should a recommendation be made for what a security policy would be?

Make no recommendations in BBA BCP

Maybe add this to the Security BCP

Travis will suggest text

Next steps, target WGLC in December

OAuth 2.0 Security Best Current Practice (draft-ietf-oauth-security-topics)

Work on a PKCE Chosen Challenge Attack

Draft is in WGLC since June

Received feedback

People/orgs are using the BCP, FAPI, PSD2, HELSEID, Cloud Signature, JS Libraries

Next steps, include rework and reorganize, add text to make PKCE mandatory for AS

Issue to state that you MUST NOT USE IMPLICIT Flow, some support this. Other do not

Humm was in favor of keeping the SHOULD NOT and not making this a MUST NOT

OAuth 2.0 Demonstration of Proof-of-Possession at the Application Layer (DPoP)

Draft proposal for PoP for access and refresh tokens

Lots of other efforts in past to solve this problem

Make something better than bearer tokens

Need a widely adopted PoP method

Status of Token Binding is in doubt, the proposal uses some of the concepts for Token Binding

Annabelle: Would you consider using a HTTP signing solution and not do this

John: This work would most likely finish before the general HTTP signing, this has limited aspirations than the http signing

OAuth 2.0 Client Intermediary Metadata

Skipped.

OAuth Security Workshop 2020

22-24 July 2020 in Trondheim Norway

https://osw2020.com

SESSION II

TxAuth BoF Summary

See TxBof Notes …

More futures discussions:

Discussion on where the discussions should take pace, new list or OAuth

Some folks feel that there is new work to do, some folks think there is not, so the BoF had no conclusion. Oauth2 work would not slow down.

Work on any future version of OAuth is long term, this should be the message

Justin to take point on what a proposal next OAuth would be, he will post to TXAuth list

OAuth 2.1 Summary

Main concern is no breaking changes to core, as there are things in the BCP that would break current implementations, so more to discuss

Maybe a BIS document may be a better approach, more discussion to be had, discussions about having 2.0 and 2.1 (2.0 +BCP, no new features).

There is still no decision on if breaking changes will be allowed, or new features

DPoP

Continued from 1st session.

DPoP proof, in the HTTP header

What is the threat model that we are trying to solve with DPoP, are we just creating yet another bearer token?

Some discussions on symmetric vs asymmetric encryption and Annabelle is concerned about the scaling and crypto costs. So some folks want both types, this would increase the scope of the effort

The scope was to be able to use something with sender constraint for SPA, this is not for broader usage, so this is limited scope not doing what HTTP Signing would be used for. So this needs to be presented as a very focused effort.

So is this a OAuth next line item with all the bells and whistles?

Clarify the scope of this proposal for a specific usage like PKCE

Lets not constrain the usage as there are use cases for other flows.

Mike: The usage of TLS for sender constraint is not deployable

Pushed Authorization Requests

No integrity and authenticity for JWT but Secured Auth request (JAR) solved this issue

So this effort is a small enhancement to JAR to push the request to the authorization endpoint

Advantages

- Can handle larger payloads
- Significant improvement in security
- Easy for client developers with simple migration path
- Easy to implement for AS developers
- Even higher-level security by passing signed/encrypted requests

Annabelle no brainer to adopt this work, can this be combined with device flow, Annabelle will look into this

Revision 01 is based upon work in FAPI

Rich Authorization Requests

Complex authorization data needed in a request, large amount of data, transaction specific data.

This is in the 03 revision, positive feedback,

Torsten want this adopted, 6 non authors have read this, so call for adoption will go out to list

OAuth and Claims

Lifts Openid claims concepts

Explains how to use this outside of Openid

Using essential concept for OpenID

Claims Sink

Authorization flows look like OpenID, code and implicit, ROPC and CC

Maintains compatibility with OIDC

Arron thinks this is the wrong approach

There will be the possibility of a virtual interim meeting.