OAuth WG Interim Meeting - AS Issuer Identifier in Authorization Response

Date

December 7th, 2020

Notes

Note taker: Justin Richer

Agenda-bash

Topic: AS Issuer Identifier in Authorization Response

draft-meyerzuselhausen-oauth-iss-resp

Presentation from Karsten

What are mix-up attacks?

- goal to steal code/token, trick client to talk to an attacker's AS
- client must support multiple AS's
- variants exist for different grants and for OIDC

variant 1: attacker can manipulate first request

- attacker replaces client ID to point to honest AS after starting at attacker's AS
- redirect code issued to client, client sends token request to attacker's AS

Defending against mix-up attacks

started at oauth security workshop in 2015

- discussion has been refined/expanded since then

are confidential clients safe?

- no: client secret is not compromised for attack to work

does pkce help?

- no: makes the attack more complicated
- attacker has to convince client to use same verifier

core of mix-up attacks: auth response always comes from honest AS

idea: add a source identifier to auth response

existing approach

- client uses separate redirect URI for each AS
- AS matches full URI (no variable parts)
- clients match URI of auth response against that AS's redirect URI
- problems:
    - requires a lot from the client
    - redirect URI must be unique for combo of auth endpoint + token endpoint
    - doesn't work for centralized registration
    - can be circumvented by dyn reg + impersonation

solution details: iss parameter

AS must provide an identifier but it's implementation-specific how to get it

- static documentation
- AS metadata

client must compare the returned parameter with the expected one

- client must not allow multiple AS's to use the same identifier

metadata includes flag to show support for extension

security considerations

is it secure? most likely!

should it be integrity protected

- you can but it's not necessary for mix-up protection

correlation with JARM

- if you already have it in the response (ie: id_token responses, JARM) you don't need need to include it again
- but additional processing: client has to reject responses where issuers don't match

security BCP mentions options

- explaining redirect uri restrictions is complicated
- goal to make 'iss' parameter more prominent

next steps

WG adoption? More feedback?

Discussion

how many have read the draft?

- Torsten, Joseph, Dominick, Aaron, Brian (prior version).
- Justin has not read the draft but is familar with the concept.

taka (Authlete):

- has been implemented, but not merged back into product yet
- conformance suite has not been updated to incorporate it
- hopes that we can see this move forward

Justin:

- what are the failure modes? if a parameter is expected and not included, or not expected and included?
- we have some experience with PKCE as a model for extension support

Denis:

- why is solution not discussed (or referenced) in the security issues draft?
- if you check the client_id (?)

Daniel:

- assumes that client has multiple client IDs to differentiate between different AS's
- but client_id @ attacker AS could be the same as at honest AS, so not a defense

Vittorio:

- is this required in the access token?

Daniel:

- This is for the client to check, so that's not part of the token

Joseph:

- "isn't the issuer thing a bug in the conformance suite?"
- this is about the OIDF FAPI/OIDC conformance suite
- it's a warning when the AS returns a parameter the suite doesn't know about
- clients should ignore it
- but additional parameters are to flag potential strange things
    - seen error responses with auth codes
    - seen user IDs with error codes
    - so conformance suite reports them with warnings

brian:

- expired working group draft: oauth mix up mitigation
    - https://tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01
- how do we handle this?

Adoption call

strong support from call attendees, will be confirmed on the list
(Brian Campbell, Torsten Lodderstedt, Dominick Baier, Daniel Fett, Aaron Parecki, Joseph Heenan, Karsten Meyer zu Selhausen, Takahiko Kawasaki, Vittorio Bertocci, Peter Yee)

Attendees

- Rifaat Shekh-Yusef
- Peter Yee
- Justin Richer
- Karsten Meyer zu Selhausen
- Daniel Fett
- Takahiko Kawasaki
- Anthony Nadalin
- Brian Campbell
- Roman Danyliw
- Hannes Tschofenig
- Joseph Heenan
- Aaron Parecki
- Torsten Lodderstedt
- Bob Horvath
- Vittorio Bertocci
- Denis
- Dominick Baier
- Melissa King
- Michael Peck
- Tim Cappalli

Document(s)

https://datatracker.ietf.org/doc/draft-meyerzuselhausen-oauth-iss-auth-resp/

Recording

https://ietf.webex.com/webappng/sites/ietf/recording/7d5b88a3a8b74f85a99dd4bcbd756dca/playback