Details for today's meeting can be found at
https://datatracker.ietf.org/meeting/interim-2020-oauth-07/session/oauth

WebEx recording can be found at
https://ietf.webex.com/recordingservice/sites/ietf/recording/playback/e33681b0bb2044df81ae78b2be9f4c1e

Agenda

1. Demonstration of Proof-of-Possession at the Application Layer
   https://datatracker.ietf.org/doc/draft-ietf-oauth-dpop/
2. Incremental Authorization
   https://datatracker.ietf.org/doc/draft-ietf-oauth-incremental-authz/

Attendees

1. Hannes Tschofenig
2. Rifaat Shekh-Yusef
3. Brian Campbell
4. Aaron Parecki
5. Andreas Falk
6. Annabelle Backman
7. Arnar Birgisson
8. Bhupinder Singh
9. Brock Allen
10. Daniel Fett
11. David Waite
12. Denis
13. Dick Hardt
14. Fabian Hauck
15. Filip Skokan
16. George Fletcher
17. Janak Amarssena
18. Jared Jennings
19. Justin Richer
20. Matt de Haast
21. Mike Jones
22. Nikos Fotiou
23. Peter Yee
24. Phil Hunt
25. Tim Cappalli
26. Vittorio Bertocci

27. Wiliam Denniss
28. Dominick Baier
29. John Bradley
30. Torsten Lodderstedt

Demonstration of Proof-of-Possession

Brian Campbell presenting

Overview

Simple and concise approach to proof-of-possession

00 WG draft published on April 1, 2020
01 published on May 1, 2020

- More formally defined the DPoP authorization header scheme
- Define the 401/WWW-Authenticate challenge
- Added invalid_dpop_proof error code
- Fixed up and added IANA section
- Added dpop_signing_alg_values

Open Questions

1. Thread Model & Objectives
    a. May not be entirely clear
    b. But sometimes also may be overly specific
    c. It is a bit of a Rrschach test
    d. Honestly, I'm hoping Dr. Daniel Fett can help here
2. Attacker Model
    a. Misconfigured Resource Endpoint
        i. DPoP protects the access token in this scenario
    b. Additional attack vectors will be posted to the list or discussed at a later time
3. Dick Hardt: is a new JWT format being defined?
    a. Brian C: No. It adds a CNF to the existing JWT format/scheme.
    b. Dick Hardt: It would seem to make sense to move the DPoP outside of the JWT so that it can be left alone. (Detached)
    c. Daniel F: DPoP is supposed to work in the same way the access token. It's a nice way to tell the resource server. The Introspection method can still be used.
    d. Justin R: Has implemented DPoP using an opaque value.

    e. Annabelle: It is possible for an entity to become confused and proposes a DPoP token as a bearer token, incorrectly. Like in a downgrade attack vector.
    f. Andrewas F: Believes additional clarification is required.
4. Difficulties with ‘jti’
    a. Can be difficult detecting/preventing replay
5. ‘Iat’ can also limit replay window
6. Open Options / ideas
    a. Explicitly mention that the replace space is qualified by the URI
    b. Further loosen/qualify (like perhaps a MAY)
    c. Drop the tracking requirement all together
7. Signal that the RT is bound?
    a. Useful to signal that the refresh token is bound
    b. Today, Refresh Tokens are only bound for public clients
8. Client metadata?
    a. What issues does this solve or how does it help?
9. How can Downgrades, Transitional Rollout & Mixed Token Type deployments be addressed?
10. Filip Skoken: The DPoP design wasn’t to change the existing scheme, but if DPoP is available the resource server can use it.

Incremental Authorization

William Denniss

Recap

- Asking for the kitchen sink up-front is a bad thing
- Users should have context to the authorization request
    - E.g. granting a calendar scope only make sense in the context of interacting with a calendar-related feature

Overview

- The ability to request additional scopes in subsequent requests adding to a single authorization grant representing all scopes granted so far.
    - Implies that the access and refresh token carry the union of all granted scopes
- Confidential Client Protocol
    - Auth 2.0 doesn’t stop you returning an authorization grant with *more* scope

    - New parameter: include_granted_scopes
    - Documents best practices
- Public Client Protocol
    - New token endpoint param: existing_grant - pass the previous refresh token in existing_grant
    - Resulting access and refresh token will include the union of scopes

Updates

1. Clarified RFC8414 metadata field
2. “Scope” response param behavior documented
3. New error code defined “overbroad_scope” that the authorization server can use this
4. Documented recommended client behavior if the user reduces scope

Open Question

1. Two ways to document for incremental auth are currently split by “public”, “confidential”.
    a. Annabelle: “public”, “confidential” definition - can the client authentication/does it have credentials that it can keep secure. This shouldn’t be confused with native vs. public apps vs. apps that have a backend.
    b. Dick H: Public/confidential the intent was to protect the authorization and that the client could keep a secret.
2. Par may help address the public/confidential challenge
3. Torsten: Granted Scopes, doesn’t ensure that it will use the existing and the new. The text reads “SHOULD” instead of “MUST”.
4. Annabelle: The AS MUST treat the previously authorization granted scopes as having been granted.

Wrap-Up

- Annabelle: Should we have additional working sessions covering DPoP?
    - Brian C and Daniel F +1