Distributed OAuth

ietf-oauth-distributed

Dick Hardt
IETF 103, Bangkok
November 2018
Distributed OAuth Refresher
AS Discovery Problem

- OAuth 2 presumes **static relationship** between authorization server and protected resource that is **known a priori** by client.
- Global systems have similar protected resources, that are managed by different authorization servers. Eg. different geopolitical regions.
- Large, distributed systems need to evolve the relationship between authorization servers and protected resources.
- Clients need to **dynamically** learn the authorization server for a given protected resource **at run time**.
Client Accessing Global Protected Resources

.cn

Authorization Server

S3

EC2

.us

Authorization Server

S3

EC2

.eu

Authorization Server

S3

EC2

Client
Access Token Reuse

- Client accesses resource server it was not granted access to
- Resource Server reuses client’s access token at another resource server
- Solution:
  - Audience restricted access token
Audience Restricted Access Token

Client

token.CN

token.US

token.EU
Discovery
HTTP 401 response

- Client discovers Authorization Server
- Client discovers resource identifier

HTTP/1.1 401 Unauthorized

    WWW-Authenticate: Bearer ...

    Link: <https://api.example.com/resource>;
        rel="resource_uri",
    <https://as.example.com/.well-known/oauth-authorization-server>;
        rel="oauth_server_metadata_uri"

- Client confirms resource URI in host and path
Access Token Request

- Client includes resource identifier in request per ietf-draft-resource-indicators

grant_type=client_credentials
&scope=example_scope
&resource=https%3A%2F%2Fapi.example.com%2Fresource
Access Token Includes Resource Identifier

- If JWT, “aud” includes resource identifier
- Resource server checks resource identifier is in access token
ietf-draft-distributed-oauth-01

- Reference ietf-draft-resource-indicators for resource identifiers
Distributed Oauth

Open Issues
Discovery

- Link headers vs www-authenticate header

- Existing libraries use www-authenticate
  - extra attributes allowed per RFC 6750

- Consensus?
AS discovery

- Currently full URL
- Change to just issuer value, and discovery per 8414
- Consensus?
Resource URL / URI

- Confusion on relationship
- ‘resource identifier’
  ietf-draft-resource-indicators
- ‘resource URL’
  URL client is calling
Next Steps

- Update draft