Authorization for IoT using OAuth

draft-seitz-ace-oauth-authz-00

Ludwig Seitz (ludwig@sics.se)
Göran Selander (goran.selander@ericsson.com)
Erik Wahlström (erik.wahlstrom@nexusgroup.com)
Samuel Erdtman (samuel.erdtman@nexusgroup.com)
Hannes Tschofenig (hannes.tschofenig@arm.com)

IETF ACE WG meeting
November, 2015
This draft

• Merge of two proposals
  – ACRE
    • draft-seitz-ace-core-authz
  – OAuth
    • draft-tschofenig-ace-oauth-iot
    • draft-wahlstroem-ace-oauth-introspection
Design Principles

1) Allow security at different layers
2) Allow different authorization schemes
3) RESTful transfer of authorization information
4) (*New*) Build on existing authorization protocols
   - OAuth 2.0 (profiled for CoRE)
   - Building blocks: CoAP, CBOR, COSE, OSCOAP
Basic OAuth Flow

- Different deployment scenarios
- Not all steps in every scenario
Profiling OAuth 2.0 for CoRE

• AS support for setting up Communication Security
  – Establish security context and security protocol C ↔ RS
• Resource for sending access tokens to RS
  – For provisioning the token independently of the request
• Authorization Information Format
  – Interoperable format for access control data in tokens
• CBOR instead of JSON
  – More compact tokens and client information
• CBOR Web Tokens
  – Compact variant of JSON Web Tokens (JWT)

→ Enable the different constrained scenarios
Example:
RS has intermittent connectivity

Token needs to be self-contained, i.e. RS can evaluate it offline
Example:
C has intermittent connectivity

- A + B done when client has connectivity, e.g. at commissioning
- Token may be a reference (i.e. does not encode specific rights)
Advantages

• OAuth already an IETF standard
  – Well-established
  – Widely deployed
• Interoperable (Internet ↔ Internet of Things)
• Compatible with existing IAM frameworks and policies already used with other OAuth deployments
• Optimized to meet CoRE constraints
Next Steps

• Details of OAuth profiling
• Check integration with OMA LWM2M
Thank you!

Questions/comments?