Highlights from the IETF ACE WG

Olaf Bergmann, **Stefanie Gerdes**, Carsten Bormann

T2TRG Meeting Breakout B, 2015-07-18

Authentication and Authorization for Constrained Environments (ACE)

- WG formed on 2014-06-16
- Goals
  - Fine-grained **authorization** on constrained clients and servers
  - Focus on REST-based architectures
- Objectives
  - Look at existing technologies
  - Identify what is needed to support constrained devices
  - Focus on CoAP and DTLS in the beginning
- Tasks
  1. Produce use cases and requirements
  2. Identify authentication and authorization mechanisms suitable for resource access in constrained environments.

Current Status

- One working group item: draft-ietf-ace-usecases
- Discussion on actors in the ACE architecture: draft-gerdes-ace-actors
- Various input that may be relevant for solution(s)
  - Use cases: draft-rahman-ace-public-safety-use-case, draft-somaraju-ace-multicast, draft-yang-ace-groupauth
  - Integration with existing (Web) infrastructure: draft-maler-ace-oauth-uma, draft-gerdes-ace-dcaf-examples
  - Protocols and protocol flows: draft-gerdes-ace-dcaf-authorize, draft-cuellar-ace-pat-priv-enhanced-authz-tokens, draft-seitz-ace-core-authz
- Object security
  - Look beyond *Coap+DTLS*
  - Closely related to IETF WG COSE (= JOSE - json + cbor)
  - Data formats: draft-ietf-cose-msg
  - Protocols: draft-selander-ace-object-security

Toolbox

- Key exchange: draft-hardjono-ace-fluffy, draft-schmitt-ace-twowayauth-for-iot, draft-gerdes-ace-dcaf-authorize, draft-somaraju-ace-multicast
- OAuth compatibility: draft-wahlstroem-ace-oauth-introspection, draft-maler-ace-oauth-uma, draft-gerdes-ace-dcaf-examples
- Data formats: draft-bormann-core-ace-aif, draft-gerdes-ace-dcaf-authorize, draft-tschofenig-ace-oauth-iot, draft-tschofenig-ace-oauth-bt,
- Group communication: draft-somaraju-ace-multicast, draft-yang-ace-groupauth

Status Summary

- High-Level
  - Use-Cases seem to largely cover the problem space
    - (But: More reviews needed!)
  - Agreement on terminology and architecture
  - Relationships of actors in the architecture
- Low-Level
  - Lots of tools for constrained applications are available for authentication and authorization?

(Some) Open Questions

- For any tool T: Where and to what extent does this tool help to solve a problem stated in draft-ietf-ace-usecases?
- What is missing from the perspective of other consortia, e.g. W3C WoT IG?
- For any use-case U: What protocol flow can be used to solve (aspects of) use-case U with the existing tool set?
- What protocol elements, interfaces, are missing to solve use-case U?
- Which interoperability requirements exist for *your* favorite scenario?