W3C IG on Web-of-Things **Security&Privacy: Plugfest Findings and Implementers Feedback**

Oliver Pfaff (ed.)
(oliver.pfaff@siemens.com)

Testing

1. By default security-enabling will be tested with the **ThingWeb client**
2. If your resource server aka servient is security-enabled please provide:
    1. One or more **URLs** pointing to **protected resources** i.e. enforce the presence of a security token
    2. Info is this demands a “**minimal**” or “**normal**” security token
    3. If requiring a “normal” token info about expected parameters **rsId**, **rId** and **mths** e.g.

        ```
        grant_type=client_credentials&
        rsId =coaps://rs.company-s.com:9684&
        rId =/trafficlight/value&
        mths=GET PUT
        ```

Findings

1. The security token form-factor **CWT** was **unavailable** due to lack of signature/encryption support in current CBOR libraries
2. The security token form-factor **JWT** is versatile but lacks a standard way of **distinguishing different types**
3. **CoAP** lacks adaptation of the **HTTP authorization framework** (RFCs 2617/7235)
4. **CoAP stacks** lack programmatic/declarative ways of telling the runtime to enforce the presence of **valid security tokens** (for certain resources)
5. **WoT** lacks consideration on whether that should be expressed in thing descriptions (opt. item for domains that prefer a-priori strategies)
6. **OAuth** resp. **ACE** miss some coverage for **cross-domain cases**:
   - Error responses (`WWW-Authenticate` response headers for HTTP, n.a. for CoAP) lack standard items to express: expected security token type/issuer/protection
   - Token acquisition lacks support of the use case "*I am X (role=domain representative) and I am asking for a token for Y (role=domain member)*"
   - Ways of referring to resource owner domain abstractions (e.g. client_id values by which an AS knows an RS) in a cross-domain friendly way (e.g. URLs)

Feedback

1. Request/encourage **adaptation of COSE** in CBOR libraries (*goes to NN*)
2. Request/encourage the **inclusion of token type labels** as “Registered Claim Name” with an IANA registration facility for common values (*goes to IETF WGs oauth and ace*)
3. Request/encourage the **adaptation of the HTTP authorization framework** in CoAP (*goes to IETF WG core*)
4. Request/encourage the addition of a capability **instructing the runtime to enforce the presence of valid security tokens** (goes to Californium et al. authors)
5. TF-TD should consider the **optional expression of RS security-enablement**
6. Request/encourage a better **coverage of cross-domain cases** (goes to IETF WGs oauth and ace)

White-Spots

- The security-enabling of the Nice Plugfest did not cover:

1. **PoP** security model for security tokens
2. **Protected registrations**
3. Actual **end users** as system actors

- These items are candidates for a follow-up Plugfest