Internet of Things Gateway Access Control

Athens University of Economics & Business
Msc Student
Stefanos Plastras

Contents

- Thesis Motivation
- Background (IoT, openHAB, OAuth2.0, JWT)
- Smart Home Frameworks - Related Work
- System Design
- Results & Evaluation
- Conclusion
- Future Work

Components (Services/Roles)

- openHAB v2.5 as a Smart Home Automation Framework
  - openHAB IoT Gateway
- ContronThings as OAuth2 Authorization-Authentication service
- Json Web Token (JWT) as data exchanged between Client – ControlThings/Proxy Server
- HTTP messages proxy service (IAA module)
- Admin (Role) access: Add/Edit/Remove Things, Register Client/Resource, Bind Client with Resource(s)
- Client (Role) access: Execute HTTP requests causing a desirable action (eg, turn on led light). Must prove to system he is authorized to access these HTTP requests

openHAB Home Environment

Admin

1. Create Client – 2. Create HTTP resource – 3. Bind Client with resource(s)

browser

4. “View” Credentials

Inform Client about credentials produced

as.controlthings.gr

6. JWT

```
{
  “access_token”:
        “eYF...Kh”
   “token_type”:
        “bearer”
    ...
}
```

5. AccessToken Request

HTTP Request
- grant_type
- client_id
- client_secret

IAA Proxy Server

conf

7. Send HTTP request requiring an action in a smart device

8. Forward HTTP request requiring an action in a smart device

9. HTTP response about smart device action (eg, status update)

10. Forward HTTP response about smart device action (eg, status update)

Client

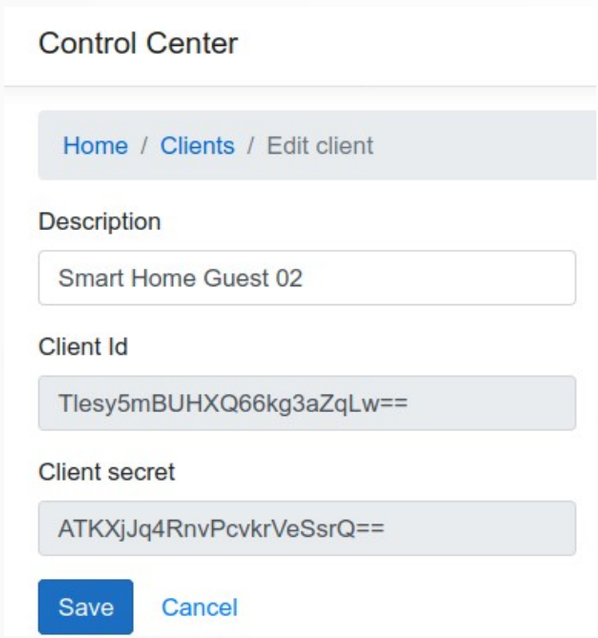
openHAB Gateway

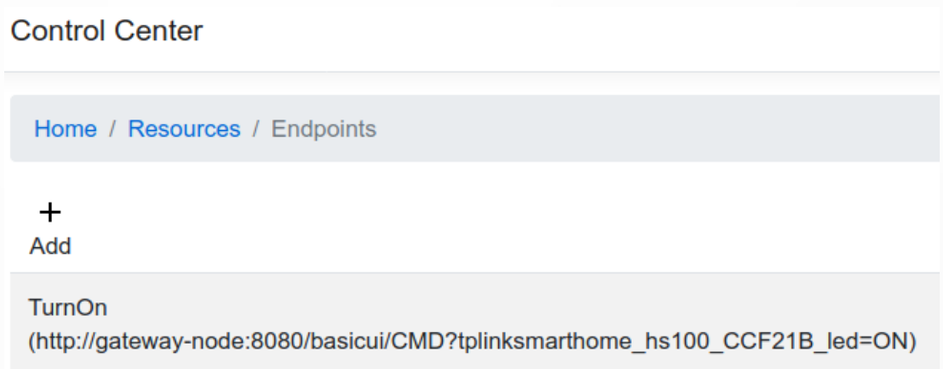
Smart TPLINK Plug

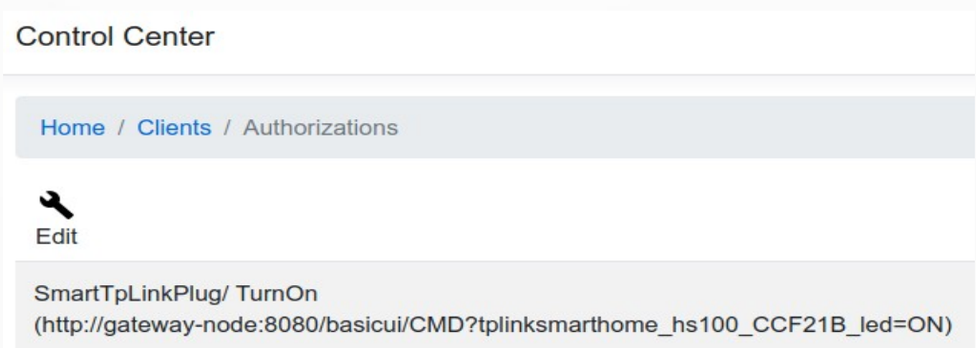
Smart LG TV webOS

Steps

- Step 1,2,3:







Steps

- Step 5:

  curl -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "**grant_type=client_credentials**&**client_id**=8S0di1q1RoHn11tdENVUEw==&**client_secret**=myClientPassword" https://as.controlthings.gr/oauth2/token/stefanos2

- Step 6 (result):

```
{
   “access_token”: “eYOplk.DfeR.LpS”,
   “token_type”   : “bearer”,
   “expires_in”    : 3600,
   “refresh_token” : “Atz|EXAMPLEREFRESHROKEN12X”
}
```

Steps

- Step 7:

  curl - curl -X GET -H "Accept: application/json" -H "Authorization: **Bearer eYOplk.DfeR.LpS** http://proxy-node:9000/basicui/CMD?tplinksmarthome_hs100_CCF21B_led=ON
  [turn on plug led]

- Step 8: Forward HTTP request of Step 7 to openHAB Gateway
- Step 9: Response about HTTP request (eg, 200 code)
- Step 10: Proxy forwards response of Step9 back to Client

Proxy Configuration (conf)

- File containing protected resources descriptions

  - Assume Client wants to turn on led by requesting it from Proxy: http://proxy-node:9000/basicui/CMD?tplinksmarthome_hs100_CCF21B_led=ON

  - Pure turn_on led request (openHAB URL → basicui/CMD? tplinksmarthome_hs100_CCF21B_led=ON)

  - Define header in conf with name <basicui/CMD>

- Also, define openHAB Gateway IP and port, signing keys path, token type.

openHAB Gateway Configuration

- Enable firewall service
  - Allow only HTTP traffic from/to Proxy Server
  - Allow SSH service for management purposes

Token Validation

- Proxy Server (IAA) offers token validation service in order to ensure that Client is indeed authorized to access the desired HTTP Resource (resource must exist in token, payload data)
- For example, this token “**eYOplk.DfeR.LpS**” (encoded)

  Payload Data (decoded)


```
{
  "sub": "Tlesy5mBUHXQ66kg3aZqLw==",
  "resources": "http://gateway-node:8080/basicui/CMD?tplinksmarthome_hs100_CCF21B_led=ON",
  "nbf": 1598894149,
  "exp": 1598980549,
  "iat": 1598894149,
  "iss": "https://as.controlthings.gr",
  "aud": "stefanos2"
}
```


- One criteria is the HTTP RESOURCE existence is Payload

How openHAB uses access token

- openHAB **does not** interact/use token in a **immediate way** (Does not accept an authorization header?)
- Consequently, proxy server is responsible for interacting with tokens (accepting, validating)
- Integration of openHAB + External System

Similar Approaches

- Official openHAB does not support Authentication, Authorization!
- Still, best option is a proxy service
- No solution in terms of Authentication, Authorization

  [Security Analysis of Open Home Automation - IEEE]

  [Scaling Home Automation to Public Buildings: A Distributed Multiuser Setup for OpenHAB 2 - IEEE]

THANK YOU FOR YOUR ATTENTION!

Now please any Questions?