Dynamic Authorization and Consent in an IoT Ecosystem Dedicated to Healthy Ageing

C. Kassapoglou Faist, D. Vizár

A dynamic authorization framework enabling fine-grained, dynamic access control has been implemented using open-source software and tools. Developed in the context of a large IoT ecosystem for the wellbeing of the elderly, it offers a solution for providing consent, thus enhancing data protection.

The Internet of Things (IoT) has opened tremendous opportunities to enhance the quality of life in a variety of domains. Among others, it offers smart remote monitoring of health indicators, enabling senior citizens to live independently longer at home, with substantial individual and societal benefits. This is the main objective of the H2020 EU Large Scale Pilot project ACTIVAGE, which establishes a European IoT ecosystem extending over nine deployment sites (DS) across the continent, responding to the needs of the elderly, caregivers, service providers and public authorities. In order to realize the ACTIVAGE IoT ecosystem, the project envisions the reuse and scaling up of existing IoT platforms (e.g. frameworks such as Fiware, Sofia, SensiNact, Universaal, openIOT), providing interfaces for interoperability including semantics.

IoT ecosystems present inherent security and privacy risks. In this report, we focus on the implementation of authorization and access control as a security function. The results are twofold: a) a dynamic authorization mechanism has been established, controlling access to the semantic interoperability layer services running above each DS IoT platform in a highly flexible way, and b) the protocols and tools used offer the possibility to a user/data-owner of the platform to manage consents and to control the access rights to his/her private data.

In its essence, the problem is the following. 1) Resources (data, metadata, services, software components etc.) within a distributed environment that are accessible as web applications (an API over HTTPS) must be protected by restricting access. 2) Access rights are determined based on rules (authorization policy, permissions) that may vary in time. Consumers of resources in a distributed environment may be physical persons ("users", using a browser) or other applications ("clients") that act on behalf of a user. Users may be data owners or other requesting parties (e.g. a data analyst).

A typical approach is to place the resources behind Resource Servers (RS - the Policy Enforcement Point-s), and delegate the access decisions to a unique Authorization Server (AS - the Policy Decision Point). Several protocols have been proposed to deal with authorization, often building on the OAuthv2 and OpenID Connect frameworks, which offer identity-based user authentication (log-in), allowing single sign-on through the use of access tokens, signed by the AS and verified by the RS before granting access to a service.

For higher flexibility and scalability, ACTIVAGE targets dynamic authorization, which is characterized by: a) fine-grained rules (best achieved by Attribute-Based Access Control); b) centrally-managed rules (decisions externalized to a single decision point); and c) real-time decisions. The User Managed Access (UMA) protocol by the Kantara Initiative [1] is a good choice to achieve this. UMA distinguishes the roles of the resource owner and the requesting party and it defines an API dedicated to resource servers (Protection API) for resource registration, permission information retrieval (permission tickets) and token introspection (verification). In addition, it exposes a UMA Grant Token Endpoint to the client, where Requesting Party Tokens (RPT) can be retrieved. Underlying to these interactions is OAuth2, assuring that the RS or the client act on behalf of a person that has been authenticated by the AS.

We used open-source tools to implement this scheme. Specifically, the AS is a Keycloak (KC) server, while the RS is empowered by an Express Gateway (EG) API server [2]. In addition to classic authentication endpoints (e.g. OAuthv2), Keycloak exposes APIs for UMA-compliant authorization services, enabling the protection of resources using ABAC. We used the KC authorization services user interface to specify the ACTIVAGE interoperability layer services as protected resources and define the rules that govern their access (in our example, role attributes were used). On the other hand, benefitting from the ability to customize EG at a very high level, we defined intermediate actions and conditions in the HTTP(S) request/response flows. In this work, we have substantially benefited from open-source software published by the KC and EG communities (Apache2 licenses). Figure 1 depicts the UMA-based authorization workflow being tested in the project.

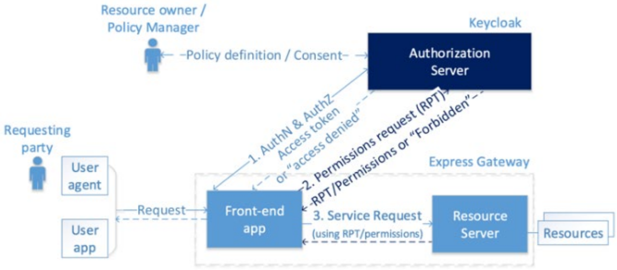

Figure 1: UMA-based dynamic authorization workflow.

Beyond dynamic rules, the UMA workflow and the KC authorization services enable the resource owner to manage fine-grained consent, asynchronously with respect to service runtime. The rules governing the data protection policy of one of the ACTIVAGE deployment sites were defined in KC in order to protect the personal data of the elderly. On top of obvious role-based rules, we added targeted consent in our working example (e.g. a specific user is entitled to see her parent's medical data) and thus test how consent can be enforced, without requiring data owner approval during the service rendering time.

With data protection gaining ever growing importance, this work has enabled us to gain valuable experience using a scalable dynamic authorization framework in an IoT ecosystem. This framework offers a complementary method to cryptographic security that can be applied at most levels of an IoT ecosystem, supporting consent and enhancing data protection.

[1] https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html

[2] https://www.keycloak.org, https://www.express-gateway.io/