An ABAC Framework for IoT Applications, Utilizing the OASIS XACML Standard

Vedran Semenski
Instituto de Telecomunicações, DETI,
University of Aveiro, Aveiro, Portugal
vedran.semenski@ua.pt

***Abstract* - IoT (Internet of Things) is an area which offers great promise and although a lot of core problems already have satisfactory solutions, security has remained somewhat unaddressed and remains to be a big issue. Access Control is a way of enforcing security that involves evaluating requests for accessing resources and denies access if it is unauthorised, therefore providing security for vulnerable resources. Access Control is a broad term that consists of several methodologies of which the most significant are: IBAC (Identity Based Access Control), RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control). In this work ABAC will be used as it offers the most flexibility compared to IBAC and RBAC. Also, because of ABAC's adaptive nature, it offers longevity and lower maintenance requirements. OASIS (Organization for the Advancement of Structured Information Standards) developed the XACML (eXtensible Access Control Markup Language) standard for writing/defining requests and policies and the evaluation of the requests over sets of policies for the purpose of enforcing access control over resources. It is defined so the requests and policies are readable by humans but also have a well defined structure allowing for precise evaluation. The standard uses ABAC. This work aims to create a security framework that utilizes ABAC and the XACML standard so that it can be used by other systems and enforce access control over resources that need to be protected by allowing access only to authorised subjects. It will also allow for fine grained defining of rules and requests for more precise evaluation and therefore a greater level of security. The primary use-case scenarios are large IoT applications such as Smart City applications including: smart traffic monitoring, energy and utility consumption, personal healthcare monitoring, etc. These applications deal with large quantities (Big Data) of confidential and/or personal data. A number of NoSQL (Not Only SQL) solutions exist for solving the problem of volume but security is still an issue. This work will use two NoSQL databases. A key-value database (Redis) for the storing of policies and a wide-column database (Cassandra) for storing sensor data and additional attribute data during testing.**

Keywords— ABAC; access control; information security;XACML; software architecture;

I. INTRODUCTION

hlgh hjg zjg gul ukl j hj [1] k

II. SECTION1

hgg hhljjičjl j

ioj čoj čoij oj jiojiojiiugtufdeswrzdiulgg zg zg dridfzć god glf ćgftfčg

III. REFERENCES

[1] "eXtensible Access Control Markup Language (XACML) Version 3.0," 22 January 2013. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf. [Accessed 4 November 2014].