Universidade de Aveiro
2015

Departamento de
Eletrónica, Telecomunicações e
Informática

Supervisor: Prof. Doutor Óscar Narciso Mortágua Pereira (omp@ua.pt)

Co-superviser: Ricardo Azevedo

An ABAC framework utilizing XACML for IoT applications

keywords:

Access Control, ABAC, XACML, JSON, IoT, Big Data, NoSQL, SMARTIE , Smart City, M2M, Security

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 security technique that evaluates requests for accessing resources and denies access if it is unauthorised therefore providing security for vulnerable resources. As Access Control is a broad term it 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 control will be used as it offers the more flexibility compared to IBAC and RBAC and because of ABAC's adaptive nature it also offers 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 utilizes ABAC. This work aims to create a security framework that utilizes ABAC and the XACML standard so that it can be utilized in other systems and enforce access control over resources that need to be protected by allowing access only to authorised subjects. It also allows for fine grained defining or 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 and etc. These application 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 utilize the use of two NoSQL databases. A key-value database (Redis) will be used for the storing of policies and a wide-column database (Cassandra) will be used for storing sensor data and additional attribute data during testing.

Vedran Semenski
vedran.semenski@ua.pt