

# Security of the Internet of Things

A contribution to the authentication, authorization, and overall security analysis of openHAB2 and Eclipse Smart Home

February 2018

## 1 Thesis project description

The Internet of Things (IoT) is a new paradigm where many smart devices, Things, gather data from their environment and share it for some kind of purpose or functionality. OpenHAB2 is a system of systems intended for the smart home environment. It integrates all sorts of devices present in a private network, and offers the means to make use of the data gathered by the Things. The data gathered by this kind of application may at times be considered to be confidential, and should not be known to other unauthorized parties. This aspect may, in fact, hinder the rapid adoption of IoT applications, even in a domestic setting. Thus, this study intends to analyze what kind of security risks may exist for the data managed by openHAB2. It is known that openHAB2 does not yet offer any means for authentication, and therefore, it is also intended to contribute to the implementation of such a mechanism, and additionally propose an access control scheme for the resources of the system.

## 2 Research questions

1. Is the data captured by Things encrypted while in transport?
2. What security threats and vulnerabilities currently exist in openHAB2?
3. How does the heterogeneity of Things impact the security guarantees offered by openHAB2?

4. What risks exist to making an openHAB2 instance open to the Internet, and how can these be mitigated?
5. How can authentication and authorization mechanisms be implemented and enforced in the openHAB2 ecosystem?

### **3 Objectives**

- Identify the current data confidentiality guarantees for sensor data in transport.
- Find the most relevant security threats and risks present in openHAB2 in two scenarios: local and external (open to the Internet).
- Implement an entity authentication mechanism and propose a suitable access control scheme for openHAB2.