Demo Abstract: Supporting Interoperability of Things in IoT Systems*

Daniele Mattiacci, Sokol Kosta, Alessandro Mei, and Julinda Stefa
Department of Computer Science, Sapienza University of Rome, Italy.
Email: lastname@di.uniroma1.it.

ABSTRACT

The Internet of the future will be of things: Large scale IoT systems integrating various technologies (tracking, wired and wireless sensor and actuator networks, enhanced communication protocols, distributed intelligence for smart objects) will change the way we live and interact with the environment. Unfortunately, a standardization for IoT systems that allows for integration of sensors, data, services and applications in a smooth way and for interoperability of different technologies was still missing.

In this work we aim at demonstrating the benefits that an Architecture Reference Model for IoT systems brings: Integration of applications, services, and various sensors in a way that is transparent to the technology. Our demo features a health-monitoring application that runs on top of the reference model. Through the functionality of the application we show how the reference model makes it easy to readily build working systems and how it supports interoperability of system components independently on the underneath hardware technology.

Categories and Subject Descriptors

[**Computer systems organization**]: Embedded and cyber-physical systems—*Sensor networks*; [**Computer systems organization**]: Embedded and cyber-physical systems—*Embedded systems*

1. INTRODUCTION

Recent advances in technology enabled the possibility for more and more devices to embed sensors and network interfaces in a cheap way. The vision of the *Internet of Things (IoT)* paradigm is to make all these devices talk to eachother like humans did within the Internet [1, 2]. Ordinary gadgets get smart and communicate with other sensors and devices to offer a whole set of new services. From when the term Internet of Things was coined in '99 in the context of a supply chain management [1], a variety of novel applications of IoT systems have been proposed. Smart cities, automated surveillance, smart transportation, ubiquitous health-care, critical infrastructure monitoring, and so on, are just a few of them [2]. These applications are feasible with the today's technology. In fact, some of them are currently deployed in small-scales. But, they feature domain-specific solutions based on protocols developed with a specific application or scenario in mind. So, we are still far from the initial vision of creating a large Internet of Things interconnecting potentially billions of sensors, devices and components. The difficulty raises because of the hardware differences of the *things* involved in these systems. In particular, they do not know how to communicate to each other, even though they are able to "talk". The domain-specific solutions developed so far, do not help in this line.

In this demo we firstly describe the Architecture Reference Model IoT-A, developed within the framework of the IoT-A FP7 project. The architecture aims at outlining principles and guidelines for the technical design of IoT protocols, interfaces, and algorithms. As a proof of concept we develop, on top of the architecture, a health-monitoring application, that we exploit to show the benefits that come from this architecture: How it allows for a seamless and smooth interoperability of various technologies, and how easy it makes it to ready build working IoT applications. We show how the various components of the IoT-A can be exploited to handle the communication and the privacy/security in the system transparently to the physical devices being used.

2. IOT ARCHITECTURE (IOT-A)

The IoT-A project defines an *Architectural Reference Model (ARM)* describing the building blocks for the standardization of the IoT systems. It proposes a standard in terms of system design components, communication and security protocols. In this section we introduce some of the main components of the model that are used in the specific application presented in this demonstration.

- Subject: In the IoT paradigm it represents any physical object that is important from a user or application perspective (a person, a device, a service, etc.). Subjects are equipped with unique identifiers (IDs). Potentially, they are equipped with a public/private key pair associated to their unique ID, used to secure communication and access restricted resources.

- RFID Tag: A small electronic device able to store in-

*This work is developed in the framework of EU FP7 Lighthouse project IoT-A: Internet of Things—Architecture (http://www.iot-a.eu/public). Contract Number: 257521.

SenSys '13, Nov 11-15 2013, Roma, Italy.

http://dx.doi.org/10.1145/2517351.2517391.

formation associated with a subject[1]. The information can be retrieved automatically by other devices using wireless technology.

- RI (*Resolution Infrastructure*): It resolves queries to object abstractions that represent physical subjects. In our IoT Architecture, the framework allows for three main functionalities to be performed on the subjects: lookup, discovery, and monitoring. Thus, a query associates a given ID with a set of information and interaction services. Information services allow querying, changing and adding information about the subject in question, while interaction services enable direct interaction with the subject by accessing the resources of the associated devices.

- AuthZ (*Authorization Component*): Whenever a subject requests access to a restricted resource this component is responsible for checking that the subject has the right permissions. The access control decision is based on Role-Based Access Control [3] and Attribute-Based Access Control [4].

- AuthN (*Authentication Component*): This module is responsible for ensuring that the identity of a subject is valid. It is mandatory for every subject to authenticate with the AuthN when entering the system, otherwise the access to resources will be limited or denied by the AuthZ component.

3. HOSPITAL APPLICATION

A very recent report of Pennsylvania Patient Safety Authority shows 813 logged wrong-patient medication errors over a six-month period in 2011[2], of which 43% occurred during the administration phase. The application we build on top of the ARM aims at avoiding these errors, often lethal to the inpatients. In our scenario inpatients are treated with medicines by nurses of the hospital. The medication type and dose are priorly decided by the doctors and are registered within the Electronic Health Record (EHR) of the inpatient.

In this demo we use the IoT-A to ensure that (1) eliminate medicine administration errors; (2) preserve the privacy of the patient by allowing only authorized personnel to access the EHR. The IoT-A based system realizes automatic data analysis before the administration phase that help the nurse to decide whether the medicine is applicable to the user or not, and in case, an alarm is raised.

3.1 Patient registration

When the patient checks in, he is given a wristband equipped with an RFID tag containing the unique ID of the patient's EHR. Similarly, every medicine in the hospital is labeled with an RFID tag which points to the electronic record containing the description of that medicine (Type, amount, expiring date, etc.).

3.2 Nurse Authentication

Nurses are equipped with TazPad devices[3], Android tablets with a built-in NFC reader, through which they read the RFID tags of both patients and medicines. When the nurse enters the patient's room with his/her TazPad device, the TazPad authenticates wirelessly with the AuthN component of the IoT-A. The protocol used to communicate with the AuthN is Http with XML syntax (see Figure 1). The authentication is a crucial step in this system, needed to ensure that the particular nurse does have the right credentials to further proceed with the medication. If the nurse has the right credentials, he/she obtains a temporary digital certificate from the AuthN to use when accessing restricted resources.

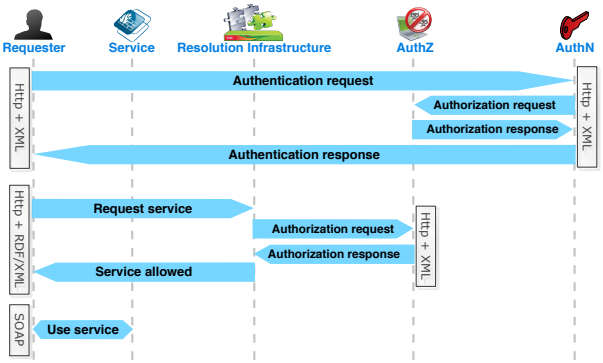

Figure 1: Interaction of system components.

3.3 Nurse Authorization

Once the nurse is correctly authenticated and comes in possession of the digital certificate, he/she is allowed to continue the medication procedure. Firstly, he/she attempts to read the patient's unique ID by positioning the NFC reader of the TazPad close to the patient's wristband. The TazPad device pulls the patient's unique ID from the patient's RFID tag, and asks the Resolution Infrastructure (RI) for the patient's EHR using Http with RDF/XML syntax for the communication. The RI asks the Authorization Component (AuthZ) to check if this particular nurse has the right permissions. The AuthZ controls if the nurse is authenticated and if the access rights for the patient's EHR can be granted. If the access control policies are satisfied, the RI allows the nurse's TazPad to be served by the responsible services. The nurse reads the EHR and selects the medicines prescribed by the doctors. After doing so, the nurse positions the NFC reader of the TazPad device close to each of the medicine's RFID label. The TazPad device sends the medicine's ID to the service in charge which pulls the medicine information from the IoT-A. Using the patient's medical history, doctor's prescription information, and medicine's information, the IoT-A helps the nurse decide whether the medicine should be administered or not. The communication between the TazPad and services follows the SOAP 1.2 protocol (see Figure 1).

4. REFERENCES

[1] K. Ashton. That "Internet of Things" Thing. *RFiD Journal*, 22, 2009.

[2] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[3] D. F. Ferraiolo and D. R. Kuhn. Role-based access controls. In *15th National Computer Security Conference*, pages 554–563, October 1992.

[4] V. C. Hu et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Technical report, NIST, 2013.

[1] http://en.wikipedia.org/wiki/Radio-frequency_identification#Tags

[2] http://patientsafetyauthority.org/NewsAndInformation/PressReleases/2013/Pages/pr_June_3_2013.aspx

[3] http://taztag.com/index.php?option=com_content&view=article&id=104