Journal of Computer and System Sciences 81 (2015) 1452–1463

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

SAFIR: Secure access framework for IoT-enabled services on smart buildings

José L. Hernández-Ramos *,[1], M. Victoria Moreno, Jorge Bernal Bernabé, Dan García Carrillo, Antonio F. Skarmeta

Department of Information and Communications Engineering, Computer Science Faculty, University of Murcia, Campus de Espinardo, 30100 Murcia, Spain

ARTICLE INFO

Article history:
Received 1 July 2014
Received in revised form 14 December 2014
Accepted 14 December 2014
Available online 23 December 2014

Keywords:
Internet of things
Smart buildings
Security framework
User-centric services

ABSTRACT

Recent advances on ubiquitous computing and communication technologies are enabling a seamless integration of smart devices in the Internet infrastructure, promoting a new generation of innovative and valuable services for people. Nevertheless, the potential of this resulting ecosystem may be threatened if security and privacy concerns are not properly addressed. In this work, we propose an ARM-compliant IoT security framework and its application on smart buildings scenarios, integrating contextual data as fundamental component in order to drive the building management and security behavior of indoor services accordingly. This framework is instantiated on a holistic platform called City explorer, which is extended with discovery and security mechanisms. Such platform has been validated in a reference smart building, where reasonable results of energy savings, services discovery and authorization are achieved.

1. Introduction

The proliferation of Internet of Things (IoT) ecosystems is radically affecting the way in which people communicate with their surrounding environment, transforming current physical spaces into real pervasive environments, in which services and resources can be accessed ubiquitously. Such scenarios are promoting a new generation of user-centric services which are provided in a huge range of environments in order to build the next generation of smart cities. Nevertheless, the realization of the resulting global ecosystem requires tackling significant security and privacy restrictions. On the one hand, physical objects are being integrated into the Internet infrastructure, making them vulnerable to attacks and misuse. On the other hand, the success of IoT services could be threatened if privacy by design or minimal minimization principles are not supported, in order to give people maximum control over their personal data.

A valuable user-centric application of smart cities is smart buildings, where people usually spend most of their time. Such pervasive environments are being equipped with sensors, smart devices and appliances that can be remotely accessed by users and services, and therefore must be protected accordingly. For this purpose, we present an integral framework which extends the security functionalities defined by the *Architectural Reference Model* (ARM) from the EU FP7 IoT-A project.[2] While

* Corresponding author.
E-mail addresses: jluis.hernandez@um.es (J.L. Hernández-Ramos), mvmoreno@um.es (M.V. Moreno), jorgebernal@um.es (J.B. Bernabé), dan.garcia@um.es (D.G. Carrillo), skarmeta@um.es (A.F. Skarmeta).
[1] Fax: +34 868 88 41 51.
[2] IoT-A: http://iot-a.eu.

http://dx.doi.org/10.1016/j.jcss.2014.12.021
0022-0000/

the integration of this framework is being realized under the SMARTIE EU project,[3] in this work we focus on authentication and authorization mechanisms to protect the access to services, as a first step to achieve a holistic security approach to be leveraged in smart building scenarios. In this direction, we propose to use localization data as an input to drive the access control for services which are deployed in typical buildings. Additionally, this framework is instantiated into a platform for services management called City explorer, which implements the main security aspects of the proposed framework while user-centric services are provided efficiently. City explorer has been validated in order to show an efficient building management, achieving energy savings, and demonstrating the feasibility of the services discovery mechanism and the main security interactions.

The structure of this paper is as follows: Section 2 reviews related works tackling user-centric services provided by smart buildings taking into account security and privacy concerns. Section 3 presents our security framework to provide a holistic approach to cope with security and privacy requirements in IoT scenarios. Section 4 presents the proposed system to manage IoT-enabled smart buildings, as well as the main involved security interactions. Section 5 presents the deployment scenario of our system as well as the validation processes carried out. Finally, Section 6 gives some conclusions and an outlook of our future work in this area.

2. Related work

With the incessant progress in the field of ICT and sensor networks, new applications to improve building management systems are constantly emerging. For instance, in office spaces, timers and motion sensors provide a useful tool to detect and respond to occupants, while providing them with feedback information to encourage behavioral changes. The solutions based on these approaches are aimed at providing models based on real sensor data and contextual information. Intelligent monitoring systems, such as automated lighting systems, have limitations such as those identified in [1], in which the time delay between the response of these automated systems and the actions performed can reduce any energy saving, whilst an excessively fast response can produce inefficient actions. Regarding building automation systems, many works extend the domotics field which was originally used only for residential buildings. A relevant example is the proposal given in [2], where the authors describe an automation system for smart homes based on a sensor network. The work presented in [3] is also based on a sensor network to cope with the building automation problem for control and monitoring purposes. Nevertheless, the authors do not propose a control application to provide user-centric services. In [4] the deployment of a common client/server architecture focused on monitoring energy consumption is described, but without performing any control action. A similar proposal is given in [5], with the main difference that it is more focused on cheap practical devices. Regarding the application of security and privacy-preserving mechanisms in the context of smart buildings, a semantic architecture is described in [6]. The proposal is developed on top of the *Open Services Gateway Initiative* (OSGi) framework and incorporates a semantic model of a smart home system. In addition, an access control policy is designed to give home owners robust control over the way users can access their devices. Moreover, in [7], a privacy dashboard is designed to improve user understanding and implementation of privacy rights related to smart buildings. Specifically, the proposed approach is based on *eXtensible Access Control Markup Language* (XACML) policies, which can be configured by non-expert users to model their privacy preferences on sensor data or actuators. However, these proposals only address the authorization stage to get access actuators and sensors data. The solution presented in [8] is based on an XACML authorization framework to get *JavaScript Object Notation* (JSON)-encoded assertions for end-to-end communication with devices. While our approach follows a similar process, we provide specific solutions for the discovery and secure access to services which are deployed in smart buildings scenarios. Additionally, these components have been integrated into a holistic platform for efficient management of services, by instantiating an ARM-compliant security framework which promotes its applicability and interoperability in a wide range of IoT scenarios in which security and privacy are required.

3. Framework for IoT-enabled smart buildings

Smart buildings can be managed following a layered and modular approach in order to provide a high-grade of interoperability throughout the different involved components. This section starts providing an overview of the main conceptual layers required to manage smart buildings environments, as well as the mapping to functional groups and components of ARM. Section 3.2 presents our ARM-compliant security framework, which is being implemented and tested in the City explorer platform under the scope of the EU FP7 SMARTIE project.[4] And finally, Section 3.3 provides an overview of the main interactions between components to provide a secure provisioning of services on smart building scenarios.

3.1. Layered overview of smart buildings environments

As can be seen in Fig. 1, three main conceptual layers can be identified in an IoT-enabled smart building environment.

[3] SMARTIE: http://smartie-project.eu.
[4] SMARTIE: http://smartie-project.eu.