Computer Networks 108 (2016) 133–147

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Security policy enforcement for networked smart objects

Sabrina Sicari[a,*], Alessandra Rizzardi[a], Daniele Miorandi[b], Cinzia Cappiello[c], Alberto Coen-Porisini[a]

[a] Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria, via Mazzini 5 - 21100 Varese, Italy
[b] U-Hopper srl, via A. da Trento 8/2, 38122 Trento, Italy
[c] Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milano, Italy

ARTICLE INFO

Article history:
Received 19 November 2015
Revised 29 March 2016
Accepted 14 August 2016
Available online 16 August 2016

Keywords:
Internet of things
Security
Data quality
Policy enforcement
Middleware
Prototype

ABSTRACT

In the Internet of Things (IoT) heterogeneous technologies concur to the provisioning of customized services able to bridge the gap between the physical and digital realms. Security, privacy and data quality are acknowledged to represent key issues to be tackled in order to foster the large-scale adoption of IoT systems and technologies. One instrumental aspect concerns the ability of the system to preserve security in the presence of external attacks. In such a scenario, the integration of a flexible IoT middleware, able to handle a large number of data streams and of interconnected devices, with a flexible policy enforcement framework is needed and presented in this paper. The proposed solution aims to ease the management of interactions across different realms and policy conflicts. Its effectiveness is validated by means of a lightweight and cross-domain prototypical implementation.

1. Introduction

The Internet of Things (IoT) [1] represents a vision of future technological ubiquity, where the ability of devices to connect to a global infrastructure enables to bridge the gap between the physical and digital realms. The diffusion of the IoT paradigm would allow the implementation and the diffusion of innovative and customized services in several applications fields. From a technological point of view, the term *'things'* is used to denote various physical everyday objects that embed electronics (e.g., wireless sensor nodes, actuators, RFIDs, and so on) to make them *smart* and suitable to be part of a global networked infrastructure. From a logical point of view, an IoT system can be characterised as a collection of smart devices which interact on a collaborative basis to fulfill a common goal, acquiring data from and acting upon the environment they are in.

In such a context, security & privacy represent critical requirements, which can hinder the large scale adoption and diffusion of IoT applications [1–6]. Traditional security countermeasures and privacy solutions cannot be directly applied to IoT scenarios due to various reasons, including, but not limited to, energy and computing constraints, scalability etc. Moreover, adaptation and self-healing play a key role in IoT infrastructures, which must be able to face sudden and unexpected changes in the operational environment. Accordingly, privacy and security issues should be treated with a high degree of flexibility [7,8]. Together with the conventional security solutions, there is also the need to provide built-in security in the devices themselves (i.e., embedded) in order to pursue dynamic prevention, detection, diagnosis, isolation and countermeasures against successful breaches [9].

Security and privacy are two pillars for ensuring the effectiveness of IoT services, the third one being data quality. IoT services should provide correct, complete and updated information: in some scenarios indeed errors or missing values might have critical impact on actions or decisions [10]. Keeping in mind the crucial role of the satisfaction of these security, privacy and data quality requirements, it is important to remark that in IoT context the number of violation attempts is high [2]. In other words, in order to deal with the huge amount of critical situations typical of the sharing approach of IoT paradigm, it is fundamental to adopt well-defined enforcement mechanisms able to successfully tackle them. Furthermore, IoT deployments are characterized by a high degree of heterogeneity in terms of architectures and technologies, so that a suitable security framework should be highly flexible in order to adapt to various deployment features.

In order to address such emerging issues, in this work we propose to integrate an existing flexible and distributed IoT middleware, called NetwOrked Smart objects (NOS) [11], with a policy

* Corresponding author.
E-mail addresses: sabrina.sicari@uninsubria.it (S. Sicari), a.rizzardi@uninsubria.it (A. Rizzardi), daniele.miorandi@u-hopper.com (D. Miorandi), cinzia.cappiello@polimi.it (C. Cappiello), alberto.coenporisini@uninsubria.it (A. Coen-Porisini).

http://dx.doi.org/10.1016/j.comnet.2016.08.014
1389-1286/

enforcement framework. More in detail, the extended middleware has to provide a policy enforcement system able to manage the resources in a secure way and to handle attacks and violation attempts. NOS is represented, in a previous work, as a security-and quality-aware system architecture [12], and is based upon the concept of a computationally powerful smart nodes' layer acting as a distributed database able to manage IoT-generated data. The basic idea underpinning NOS is of bringing processing, security and data qualification closer to the actual data sources. To ease the development of applications and the management of such a system, in [11], the NOS middleware has been designed and prototyped. It includes provisioning for users and applications to dynamically specify the levels of security and data quality suitable for their own purpose.

However, the original NOS architecture does not define supporting mechanisms for: (i) controlling the access of both users and data sources; (ii) the data provision to users. An enforcement system would allow to overcome such limitations. As regards the enforcement mechanisms, few efforts are currently made by the scientific community [2,13]. To the best of the authors' knowledge, no specific enforcement solution for IoT is currently available, although it is essential to ensure a safe deployment of IoT paradigm. To address such shortcoming, in this paper we propose a policy enforcement system specifically tailored to IoT, able to manage the interactions among the involved entities under well-defined policies. The proposed solution is able to guarantee data quality, security and privacy also in the presence of policy violation attempts.

The paper is organized as follows. Section 2 reviews the relevant state of the art. Section 3 presents the NOS architecture, with a specific focus on data management aspects. Section 4 describes the proposed enforcement framework. Sections 5 and 6 present the prototypical implementation of the NOS policy enforcement framework and its validation, in order to demonstrate the feasibility of the proposed approach in a real IoT context. Section 7 concludes the paper and provides some hints for future works.

2. Related works

The most crucial challenge in building an IoT system lies in the lack of common, standardised and interoperable software frameworks. In order to fill this gap, the scientific community has started several interesting research initiatives. For example, in recent years, the availability of web service solutions has provided a common frame for building systems able to leverage the services of another one according to the principles of Service Oriented Architectures (SOA). Service-oriented Communications (SOC) technologies emerged as a way to manage web services by creating a virtual network and adapting applications to the specific needs of users rather than forcing users to adapt to the available functionality of applications [14,15]. Although the decision of adopting SOA architecture in IoT is shared by the majority of scientific community, at the moment the state of the art in this area is mostly limited to research and innovation activities [16,17] with limited commercial uptake.

Furthermore, due to the very large number of heterogeneous technologies normally co-existing within IoT deployments, several middleware layers are employed to enforce the integration and the security of devices and data within the same information network. Within such middlewares, data must be exchanged respecting strict protection constraints. Moreover, in middleware design and development, different communication protocols shall be supported: while many smart devices can natively support IPv6 communications [18,19], existing deployments might not support the IP protocol within the local area scope, thus requiring ad hoc gateways and supporting middlewares [20]. Recent works on IoT middlewares are: VIRTUS [21], which relies on the open eXtensible Messaging and Presence Protocol (XMPP) to provide secure event-driven communications; Otsopack [22] and Naming, Addressing and Profile Server (NAPS) [23] are data-centric frameworks based on HTTP and REpresentational State Transfer interfaces. We differentiate from them since: (i) Conzon et al. [21] focus only on the application of an authentication system and on securing the communication channel by means of encryption mechanisms; (ii) Gømez-Goiri et al. [22] and Liu et al. [23] address, respectively, ambient intelligence in constrained environments and resources naming management, without dealing with security issues.

Many relevant activities have taken place within the framework of EU R&D actions. The FP7 COMPOSE (Collaborative Open Market to Place Objects at your Service) project [24] aims to design and develop an open marketplace, in which data from Internet-connected objects can be easily published, shared and integrated into services and applications. The basic concept underpinning such an approach is to treat smart objects as services, which can be managed using standard service-oriented computing approaches and can be dynamically composed to provide value-added applications to end users.

The iCORE project (iCORE) [25] aims to empower IoT with cognitive technologies and is focused on the concept of virtual objects (VOs). VOs are semantically enriched virtual representations of the capabilities/resources provided by real world objects. Through the inception of VOs it becomes possible to easily re-use Internet-connected objects through different applications/services, also supporting their mash-up into composite services. VOs provide a unified representation for smart objects, hiding from the application/service developers low-level details as well as from underlying technological heterogeneity. They also provide a standardised way to access objects' capabilities and resources. One key element in the iCORE project is the use of advanced cognitive techniques for managing and composing VOs in order to improve IoT applications and better match user/stakeholder requirements. The considered application scenarios include ambient assisted living, smart office, transportation and supply chain management.

A dynamic architecture for services orchestration and adaptation has been proposed in IoT.EST (Internet of Things Environment for Service Creation and Testing) [26]. The project defines a dynamic service creation environment that gathers and exploits data from sensors and actuators that use different communication technologies and formats. Such an architecture deals with different issues such as composition of business services based on re-usable IoT service components, automated configuration and testing of services for "things", abstraction of the heterogeneity of underlying technologies to ensure interoperability.

Focusing on semantic web services, the Ebbits project [27] designed a SOA platform based on open protocols and middleware, effectively transforming every subsystem or device into a web service with semantic resolution capability. The goal is to allow businesses to semantically integrate the IoT into mainstream enterprise systems and support interoperable end-to-end business applications.

Finally, security, privacy and trust issues are addressed by the uTRUSTit [28] and the Butler [29] projects. The former one is a project integrating the user directly in the trust chain, guaranteeing transparency in the underlying security and reliability properties of the IoT. If successful, uTRUSTit aims to enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgments on the trustworthiness of such systems. Butler aims to allow users to manage their distributed profile allowing data duplication and identities control over distributed applications. The final purpose is to implement a framework able to integrate user dynamic data (i.e., location, behaviour) in privacy and security protocols.