Information Systems 62 (2016) 29–41

Contents lists available at ScienceDirect

Information Systems

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

AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things

Alessandra Rizzardi [a], Sabrina Sicari [a,*], Daniele Miorandi [b], 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, via A. da Trento 8/2, 38122 Trento, Italy

ARTICLE INFO

Article history:
Received 26 May 2016
Accepted 27 May 2016
Recommended by: D. Shasha
Available online 4 June 2016

Keywords:
Internet of Things
Security
Publish & Subscribe
MQTT
Middleware
Prototype

ABSTRACT

The arising of the Internet of Things (IoT) is enabling new service provisioning paradigms, able to leverage heterogeneous devices and communication technologies. Efficient and secure communication mechanisms represent a key enabler for the wider adoption and diffusion of IoT systems. One of the most widely employed protocols in IoT and machine-to-machine communications is the Message Queue Telemetry Transport (MQTT), a lightweight publish/subscribe messaging protocol designed for working with constrained devices. In MQTT messages are assigned to a specific topic to which users can subscribe. MQTT presents limited security support. In this paper we present a secure publish/subscribe system extending MQTT by means of a key management framework and a policy enforcement one. In this way the flow of information in MQTT-powered IoT systems can be flexibly controlled by means of flexible policies. The solution presented is released as open source under Apache v.2 license.

1. Introduction

The Internet of Things (IoT) represents an emerging paradigm for networking and service provisioning, embracing heterogeneous devices (e.g., wireless sensor networks, RFIDs, actuators) and communication technologies in order to acquire data from the physical realm and process them in order to cooperatively provide useful services for the interested users [1]. Examples of IoT scenarios include health equipments for patients monitoring, connected cars in vehicular networks, surveillance devices, wearable sensors, smart home systems, and so on. In such contexts, it is fundamental to define how the involved "things" could efficiently communicate and exchange information among themselves and with remote servers. One key challenge relates to the amount of data generated, which poses scalability issues. Furthermore, some of such data may represent sensitive or personally identifiable information. What emerges is that there are significant issues to be addressed in order to efficiently and securely manage IoT systems. Such problems are related to: (i) the management of connections among the IoT system and the data sources (e.g., the devices which acquire information from the IoT environment), which could be affected by resources constraints in terms of energy and storage capacity (ii) the possibility, for the users, to control the distribution of their sensitive information through IoT connections as well as effective authentication and authorization mechanisms both for users and devices in order to prevent malicious access to resources [2].

[*] Corresponding author.
E-mail addresses: alessandra.rizzardi@uninsubria.it (A. Rizzardi), sabrina.sicari@uninsubria.it (S. Sicari), daniele.miorandi@u-hopper.com (D. Miorandi), alberto.coenporisini@uninsubria.it (A. Coen-Porisini).

http://dx.doi.org/10.1016/j.is.2016.05.004
0306-4379/© 2016 Elsevier Ltd. All rights reserved.

As regard the first issue, several existing application-level protocols for IoT and Machine-To-Machine (M2M) [3,4] systems have been designed. Such protocols are typically conceived to introduce little overhead and to minimize battery consumption, as well as to perform well in the presence of many short messages. The most widely adopted communication protocols for such fields are MQTT (Message Queue Telemetry Transport) [5] and CoAP (Constrained Application Protocol) [6], which are based on TCP and UDP, respectively. In our work, we focus on MQTT due to its maturity, stability and the fact that, after the recent adoption by the OASIS Consortium as official standard,[1] it is likely to become the de facto standard for IoT.

MQTT is a lightweight event- and message-oriented protocol, which allows the devices to asynchronously communicate across constrained networks to reach remote systems, as happens in a typical IoT/M2M scenario. MQTT is based on a publish/subscribe interaction pattern. In particular, MQTT has been implemented for easily connecting the “things” to the web and support unreliable networks with small bandwidth and high latency. This protocol employs a client–server pattern in which the server part is represented by a central broker that acts as intermediary among the clients (i.e., the entities that produce and consume the messages). All the communications among server and clients happen via a publish/subscribe mechanism, based on the topic concept. A topic is a mean for representing the resources (i.e., the information) exchanged within the system. Topics are used by clients for publishing messages and for subscribing to the updates from other clients. In Section 3 we analyze in depth MQTT features and functionalities and our motivations to employ such a protocol in the proposed IoT architecture. In particular, the actual version of MQTT (v 3.1.1) does not natively support neither mutual authentication mechanisms nor techniques able to guarantee the integrity and the confidentiality of the transmitted information.

Regarding the second issue, adequate mechanisms should be defined in order to control the flow of information and to enforce proper policies implementing specific rules for the management of resources and for handling users preferences. Such mechanisms should be expressive and flexible enough to support the wide range of technologies acting in IoT infrastructures and the various application domains where users and devices could operate. The aforementioned policies concern security requirements, in order to deal with different violation attempts, but also data quality aspects. More in detail, users should be aware of the levels of security and data quality of the information they receive by or transmit to the IoT system, in order to be able to filter them on the basis of personal (or, alternatively, application-dependent) preferences. As far as security levels are concerned, we consider four specific requirements: (i) data confidentiality; (ii) data integrity; (iii) privacy of the data sources; (iv) robustness of the authentication/authorization mechanisms adopted by the data sources. Concerning data quality requirements, we evaluate (i) data accuracy; (ii) data precision; (iii) information timeliness; (iv) information completeness [7].

Summarizing, in this paper we propose a new secure MQTT mechanism, named AUPS (AUthenticated Publish & Subscribe), which has been integrated in a flexible and cross-domain IoT architecture, starting from the Networked Smart Objects (NOS) middleware defined in [7,8]. NOSs are able to distributedly manage heterogeneous sources and evaluate the security and data quality of the information, in order to satisfy users' requirements and provide a lightweight and secure information exchange process. In such a system, AUPS has been further integrated with a policy enforcement mechanism, which guarantees the authentication and authorization of data sources via MQTT. AUPS is openly released under Apache v.2 license.[2]

The paper is organized as follows. Section 2 reviews the state of the art in terms of access control solutions and policy enforcement mechanisms for distributed networked systems. Section 3 describes the proposed IoT architecture, along with the adopted MQTT protocol and the proposed policy enforcement framework. Section 4 presents the integration between MQTT protocol and the enforcement mechanisms, in order to deal with security issues in the investigated context; its robustness is evaluated against possible violation attempts. Section 5 analyses a prototypical implementation of the proposed solution and presents performance evaluation results. Finally, Section 6 concludes the paper and discusses directions for future extensions and enhancements.

2. Related works

Before starting to design and develop our solution, a deep analysis of the state of the art has been carried out, with reference to both access control aspects in distributed systems as well as to the existing enforcement mechanisms. We remark that policies are operating rules which need to be enforced for the purpose of maintaining order, security, and consistency on data. A policy enforcement mechanism ensures that system operations can be performed only if they comply with the underlying security policies, typical operations be access (read or write) to resources. While security is widely acknowledged to be one of the major challenges for the wide adoption and diffusion of IoT systems [2], scientific literature on the topic is rather scarce.

For example, [9] focuses on the definition of a simulation environment supporting various policy languages, such as WS-Policy (Web Services-Policy) and XACML (eXtensible Access Control Markup Language), adopted in different systems. The final goal is to allow cross-domain policy enforcement. Note that, before applying policies across domain boundaries, it is desirable to know which policies can be supported by other domains, which are partially supported, and which are not supported. For this purpose a semantic model mapping and translation for policy enforcement across

[1] https://www.oasis-open.org/committees/mqtt.

[2] https://bitbucket.org/alessandrarizzardi/nos.