Computer Networks 112 (2017) 237–262

Contents lists available at ScienceDirect

Computer Networks

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

Review article

Access control in the Internet of Things: Big challenges and new opportunities

Aafaf Ouaddah[a,*], Hajar Mousannif[b], Anas Abou Elkalam[a], Abdellah Ait Ouahman[a]

[a] OSCARS Laboratory, Ensa of Marrakesh, Cadi Ayyad University, Marrakesh, Morocco
[b] LISI Laboratory, FSSM, Cadi Ayyad University, Marrakesh, Morocco

ARTICLE INFO

Article history:
Received 7 June 2016
Revised 5 November 2016
Accepted 8 November 2016
Available online 9 November 2016

MSC:
00-01
99-00

Keywords:
Internet of Things
Security
Privacy
Access control

ABSTRACT

In this paper, an extensive state of the art review of different access control solutions in IoT within the Objectives, Models, Architecture and Mechanisms (OM-AM) way is provided. An analysis of the security and privacy requirements for the most dominant IoT application domains, including Personal and home, Government and utilities, and Enterprise and industry, is conducted. The pros and cons of traditional, as well as recent access control models and protocols from an IoT perspective are highlighted. Furthermore, a qualitative and a quantitative evaluation of the most relevant IoT related-projects that represent the majority of research and commercial solutions proposed in the field of access control conducted over the recent years (2011- 2016) is achieved. Finally, potential challenges and future research directions are defined.

1. Introduction

Have you ever imagined your clothes, furniture, cars, household lights or even your coffee pots have their own Twitter accounts, interact with social networks and send data to the cloud, enabling aggregation of data from different devices and aspects of your lives? That is the era of The Internet of Things where the barriers between the real and cyber worlds are increasingly annihilated by turning out every day physical devices to smart objects. This is a huge and fundamental shift. When we start making things intelligent, it is going to be a great engine for creating new products and new services to improve peoples everyday lifestyle, spawn new businesses and make hospitals, factories, roads, airways, offices, retail stores and public buildings, smarter. So what will really happen when things that heretofore were blind and mute; talk, wash, hear and even think? These billions of devices are, actually, pervading our surrounding environment and even our bodies. For the sake of improving our lifestyle, they are tracking us and increasingly encroaching on our private and intimate spaces. Indeed, smart meters deduce when we shower, cars know when we do not go to work, wearable medical devices know our weight, and mobiles know how we feel [1]. As consequence, the success or failure of this revolutionary evolution will be determined by two key challenges: security and privacy. Since lack of trust about privacy will result in decreased adoption among users. Actually, a study [2] about the future of digital trust released by orange has shown that 78% of consumers think that it is hard to trust companies when it comes to use their personal data. The EU Commissions public consultation on IoT governance and the FTCs latest debates have shown in a clear way that there is an urgent need for implementing security measures for minimizing the impact of a cyber-attack and unlawful profiling and surveillance of individuals.

More specifically, in this paper, we explore access control area as one of the most crucial aspect of security and privacy in IoT. Actually, a robust security study should identify who has access to what, when and in which conditions. The Common Criteria defines an organizational security policy as: a set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment [3]. Such an organizational security policy usually relies on an access control policy [4]. An access control model is often used to rigorously specify and reason on the access control policy (e.g., to verify its consistency). However, the model does not specify how the security policy is enforced. The enforcement should be realized by technical security mechanisms, such as credentials, Cryptographic transformations (e.g., signature, encryption), access control lists (ACL), and firewalls among others.

* Corresponding author.
E-mail address: aafafouaddah@gmail.com (A. Ouaddah).

http://dx.doi.org/10.1016/j.comnet.2016.11.007
1389-1286/

Providing an adequate access control model for IoT services is a vital but challenging topic. Indeed, authentication and authorization issues have been intensively investigated through existing protocols for use cases outside constrained environments. However in constrained environments, those issues are still in their infancy. In fact, additional and different requirements pose challenges for the use of various security protocols. In particular, the need arises for a dynamic and fine-grained access control mechanism, where users/resources are constrained.

Our paper is the first, to the best of our knowledge, which surveys and focuses, in an extensive way, on access control in IoT environments, and presents in a comprehensive way models, protocols, and framework solutions in IoT. In fact, there are other surveys that have tried to address issues related to the IoT paradigm:

Maw et al. [5] deals with access control issues but only in Wireless Sensors Network (WSN) environments.

Sicari et al. [6] analyzes security, privacy and trust in IoT context but does not handle the access control issue in an exclusive way.

Atzori et al. [7] analyzes IoT enabling technologies and existing middleware solutions, and presents security and privacy open issues but it does not establish the link between the models and the mechanisms.

Miorandi et al. [8] picks out the main challenges in IoT, dealing with data confidentiality, privacy, and trust with respect to security requirements and examines the main research contexts (i.e., impact areas, projects, and standardization activities).

Weber [9] describes the security and privacy challenges but only from a legislative perspective.

Yan et al. [10] focuses only on trust management in IoT.

Roman et al. [11] explores the pros and cons of centralized and distributed architectures of security and privacy in IoT, with an analysis of the principal attack models and threats.

Gubbi et al. [12] provides a general overview of various IoT aspects, such as involved technologies, applications, cloud platforms, architecture, energy consumption and security issues, quality of service and data mining implications.

However, none of the works presented above surveys in a comprehensive way access control issue in the Internet of Things. This paper extends and improves our prior work in [13,14] with significant new materials. More specifically, our contributions can be summarized as follows:

- Definition of a reference model for comprehensively analyzing and reviewing authorization process in IoT based on the OM-AM way .
- Analysis of the main characteristics and security requirements that make IoT and its main domains application a unique ecosystem compared to previous Information Technology (IT) infrastructures. With respect to those properties, a number of security and privacy preserving objectives are identified.
- Review of the literature about access control solutions in IoT within the defined OM-AM reference model.
- Highlight for each refereed access control solution its own strengths and weaknesses.
- Elaboration of a qualitative and a quantitative evaluation: based on the fourteen identified Security and Privacy-Preserving objectives.
- Guide for the reader to know the pros and cons and the usability of current and traditional access control models and protocols from an IoT perspective.
- Extraction of the mains challenges, potential future research directions and opportunities of access control in IoT

The remainder of this paper is organized as follow: Section 2 defines the four layer of our adopted OM-AM reference model that we follow to analyze and review the authorization process in IoT. Section 3 discusses and reviews the literature for each layer separately. Section 4 evaluates in a qualitative and quantitative way the studied solutions. Section 5 extracts the main challenges of access control in IoT. Section 6 gives hints of potential and future research directions. Section 7 concludes our paper.

2. A proposed (OM-AM) authorization reference model for IoT

Access control: definition and background: Authentication and access control technologies are known as the main elements to address the security and privacy issues in the Internet of Things. Actually, any effective access control system should satisfy the main security properties of confidentiality (preventing unauthorized divulgation of resources), integrity (preventing resource to be modified without authorization resources), and availability (assuring access to resource by legitimate users when needed). More details about access control models, policies and mechanism could be found in [15]. A complete access control system covers the following three functions [16]: Authentication [17], Authorization [18] and Accountability. In this survey, we focus only on Authorization. Authentication and accountability are out of the scope of this paper.

2.1. OM-AM authorization reference model

2.1.1. Motivation

Authorization involves the following phases: defining a security policy (set of rules), selecting an access control model to encapsulate the defined policy, implementing the model and enforcing the access rules. Each phase requires specific tools to be deployed. We cite as example: Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) method [19] that can be used as a basis to derive the security policy, the RBAC model [20] to define an access control model, Extensible Access Control Markup Language (XACML) standard [21] to propose an architecture and language to implement security policy rules, and Oauth2.0 framework [22] which includes the authentication phase but proposes also an architecture (including entities and workflow) to implement the authorization function. Unfortunately, we notice a big confusion between those tools in the literature and even in the terms used in authorization field. As a result, we find an illegitimate comparison between some of the above tools and their fitness to IoT environment. That is due to the lack of a normalization of the terms used in authorization process in the literature. To fill this gap and avoid any confusion, we find that it is a worthwhile idea to propose a reference model as normalization to authorization process. By analogy to OSI (Open Systems Interconnection) 7 layers network protocol stack, we opt for the four layer OM-AM framework coined in [23], or more informally the OM-AM way, to analyze the authorization process. OM-AM stands for Objective, Model, Architecture, and Mechanism. The objective and model (OM) layers articulate what the security objectives are and what should be achieved, while the architecture and mechanism (AM) layers address how to meet those requirements. Like OSI 7 layers, each OM-AM framework layers mapping to adjacent layers is many-to-many. In other words, security policy can be formalized with many access control models as they can support different security policies. Moreover an access control model can be supported by multiple architectures, while a specific architecture can support multiple models, and do not necessarily comply with the top-down waterfall-style software engineering process.