ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/316175666

Access control in IoT: From requirements to a candidate vision

Conference Paper · March 2017

DOI: 10.1109/ICIN.2017.7899435

CITATIONS
6

READS
1,791

3 authors:

Dina Hussein
Orange Labs, Caen, France
18 PUBLICATIONS **478** CITATIONS
SEE PROFILE

Emmanuel Bertin
Orange Labs
118 PUBLICATIONS **726** CITATIONS
SEE PROFILE

Vincent Frey
Orange Labs
16 PUBLICATIONS **74** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

ITEA2 11020 SITAC Social Internet of Things – Apss by and for the Crowd View project

Towards a More Secure EMV Payment System View project

All content following this page was uploaded by Emmanuel Bertin on 06 April 2018.

The user has requested enhancement of the downloaded file.

Access Control in IoT: From Requirements to a Candidate Vision

Dina Hussein, Emmanuel Bertin and Vincent Frey*
Orange Labs
Caen 14000, France
*Rennes 35510, France
{dina.hussein, emmanuel.bertin, vincent.frey}@orange.com

Abstract— **This paper investigates the main requirements for achieving Access Control (AC) in IoT as induced from literature. A novel AC architecture is then proposed as a candidate approach for AC in IoT taking into account the addressed requirements. That is, AC is proposed to be administered at the level of IoT communities sharing common attributes, i.e. mission, location, resource capability, or device owner, etc. Thus, AC is enforced via resource-capable devices, referred to as gatekeepers, on behalf of other resource-limited nodes in a given IoT community.**

Keywords—Internet of Things (IoT); Access Control (AC); architecture; smart homes

I. INTRODUCTION

Access Control (AC) is a field in network security which entails the selective restriction of access to services, data, or for performing a certain operation on a resource, service or connected object. The decision to grant access is called authorization. In this sense, Gusmeroli et al. [1] define AC as a method for controlling who (referred to as subject) can perform which access rights (usually referred to actions) on which resource (usually referred to as object). Thus AC is represented via set of assertions involving subjects, access rights and objects [1]. Realizing AC in IoT is however understated in literature despite being essential for authorizing access to protected IoT devices, services and resources [2].

Different from its predecessors (traditional Internet, mobile Internet, sensor network, M2M, etc.), IoT mainly focuses on more ubiquitous service patterns, universal accesses for people, things, devices, services, processes, etc., on top of heterogeneous network architectures. These distinctive characteristics introduce new requirements for AC in IoT.

This paper proposes an analysis of the requirements for AC in IoT as deduced from literature. Additionally a candidate approach for meeting the requirements is presented.

II. REQUIREMENTS

A. *Thin clients and server architecture*

The concept of thin client consists in stateless client devices that rely heavily on their assigned server in order to fulfil computational activities. In the same vein, a thin server can be defined as devices that do not host any application logic. In the domain of IoT thin servers can envisions infrastructures which are independent from particular applications or security domains which is nowadays essential in future-driven IoT applications.

On another hand, AC is usually administered in a fully centralized or distributed manner. That is, in centralized AC approaches authorization decisions are carried out centrally in an application specific server prior to each access request (see Fig. 1.a). This centrality however raises concerns regarding the scalability and Single Point of Failure (SPOF) issues. In addition, it doesn't support AC in cross applications and security domains. Conversely, distributed AC architecture relies on the provisioning of a certificate or access token by a central authority which can then be used to access a device or group of devices after validating its correctness locally at the device level prior to each access request (see Fig. 1.b). However a great challenge that hinders the realization of the fully distributed AC approach is IoT objects' resource capability to validate the correctness of a given certificate or token and enforce access rights associated with it. Thus, envisioning thin client and server architecture seems well suited for AC in IoT.

B. *Autonomous & self-contained AC*

On September 22, 2016 newspapers reported: *"Behind a series of powerful computer attacks, a network of pirated connected objects."* [3]. This incident took place when a botnet of thousands of connected cameras were used to perform denial of service (DDoS) attack on the French host OVH in the period from 18 to 23 September, 2016.

This recent story raises a flag concerning the challenges for security in the IoT arena; where securing the access and usage of a vast number of vulnerable connected objects is still understudied. In fact, to protect sensitive IoT data generated by devices against cyber-attacks, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, these solutions are susceptible to many types of cyber-attacks and they do not prevent authorized entities from performing certain actions on the resources or connected objects in question. Additionally, the cryptographic methods introduce a heavy computation overhead on the device owner for key distribution and data management. Envisioning an automated and self-contained AC is therefore required in IoT.

without the need to rely on the devices' computational capabilities or having to deal with password fatigue issue, where requesting subjects need to manage an array of passwords for different applications.

C. *Infrastructure integration*

A general requirement for IoT is to support the integration with several industry players and third parties. An example to this infrastructure integration is the novel home automation solution "Celiane with Netatmo" [4] which is jointly developed by Legrand, a world-leading company in electrical installations along with Netatmo, a French company specializing in connected objects. This solution, which will be available beginning of 2018, will allow the control of a group of connected objects at home from a common controller (physical, application-based or voice controller). Additionally, users can personalize event-based scenarios. For instance, turning on the TV can set off a dim light in the living room or the opening of the front door will be able to control that of rolling shutters, etc. This example demonstrates an integrated infrastructure. That is, IoT architecture should be designed as an open framework to accommodate compatible components. Such openness seems necessary to achieve future-driven AC in IoT, by providing cross-application authorizations to services providers. This could also give a great opportunity for developers and tech-savvy to integrate their own solutions into an open AC architecture.

D. *Attributes-centric AC*

Asserting the identities of access requesters, subjects, is traditionally considered as a crucial part of AC systems. Relying on a central identity management authority to assert the identities of access requesters in cross-domain IoT applications is proposed in literature [5]. However, relying on identities for authenticating a requester before making an authorization decision seems to introduce more complexity in several IoT scenarios where IoT devices identities are hard to maintain and assert. Instead, relying on a combination of several attributes for asserting authenticity of the requester, e.g. current location, owner or manufacturer seems more reliable for AC in distributed environments. For instance, a laptop has its manufacturer model number, a product key of its operating system and an IP or Media Access Control (MAC) address. Thus, identity becomes a mere parameter in a list of attributes needed to evaluate an access request. This attribute-based authentication is necessary for realizing AC in IoT.

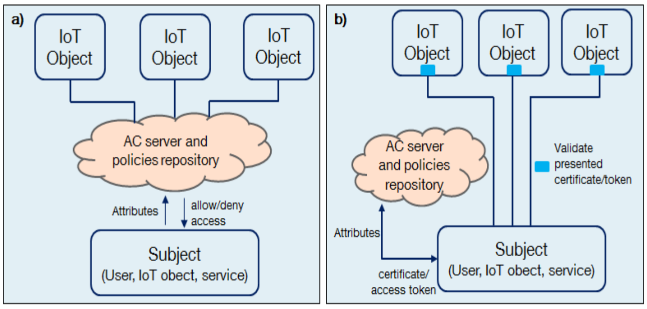
a)
IoT Object
IoT Object
IoT Object
AC server and policies repository
Attributes
allow/deny access
Subject (User, IoT obect, service)
b)
IoT Object
IoT Object
IoT Object
AC server and policies repository
Validate presented certificate/token
Attributes
certificate/ access token
Subject (User, IoT obect, service)

Fig.1. AC architecture. a) Centralized AC. b) Distributed AC

III. TOWARDS SOLUTIONS: COMMUNITY-BASED AC IN IOT

A. *Community-based architecture in IoT*

In fact, it is noticeable that the architecture of IoT is rarely flat; instead, IoT objects are usually grouped into communities sharing common attribute(s), i.e., location, mission, resource capability, manufacturer, controller, etc. The solution "Celiane with Netatmo" previously presented notably assumes a community of connected objects at home which share a common mission statement i.e., accommodating inhabitants of a smart home, and thus can be triggered or controlled centrally.

In the context of AC in IoT, the conceptualization of community as an architectural solution seems well suited, taking also into account the associated notions of rights and obligations.

The concept of community is studied within the philosophy of social science and this can bring a fresh perspective in IoT. A community is there defined as an identifiable, typically evolving and coherent grouping of people, sharing some set of usually equally evolving concerns. In the same vein, an IoT community can be composed by the following elements:

- An evolving set of objects and services, each one having a specific position within the community according to its capabilities (e.g. sensor, actuator, controller, etc.);
- A set of goals shared by these objects and services, which defines the mission statement of the community;
- A set of policies defining the rights and obligations of objects, according to their task in the community.

From an AC perspective, this conceptualization of communities is helpful to clarify the notion of access rights and obligations. In this paper, we adopt the community-based AC architecture in order to govern AC in IoT namely, COBAC.

B. *COBAC Framework*

In COBAC, first time authorization of a requesting subject is split between two parties: A certificate Authority (CA) and Application Server (AS). In which, the requesting subject will send a list of attributes (i.e., identity, location, device owner, etc.) to be verified and signed by the CA. Then these signed attributes will be presented to the AS which authorize the subject by means of a certificate, a key or token which allows the former to interact with a given community of objects (CO).

In order to actualize the authorization decision obtained by the AS we propose the role of a Gatekeeper (GK) which is responsible for actualizing and enforcing access decision at the level of CO. In which, the AS generated certificate, token or key authorizing a requesting subject to gain access to a given CO will be validated by the GK to ensure it has not been forged by third parties. Then and depending on the security policies of the requesting subject and individual devices in the CO, the GK will assign a set of rights and obligations associated with the requesting subjects. Access rights refer to the authorized access rights which can be performed by subjects towards objects in the CO i.e. read, write, execute, etc. Access obligations refer to the rights which CO objects can perform on the requesting subjects once it becomes member of the CO. In order to assign these rights and obligations, the GK will store the security policies of subjects and objects and thus generate an access matrix to assign both rights and obligations. Additionally the AS will store the CO security policies which are specified by the administrator at the design time. The COBAC framework is shown in Fig. 2.

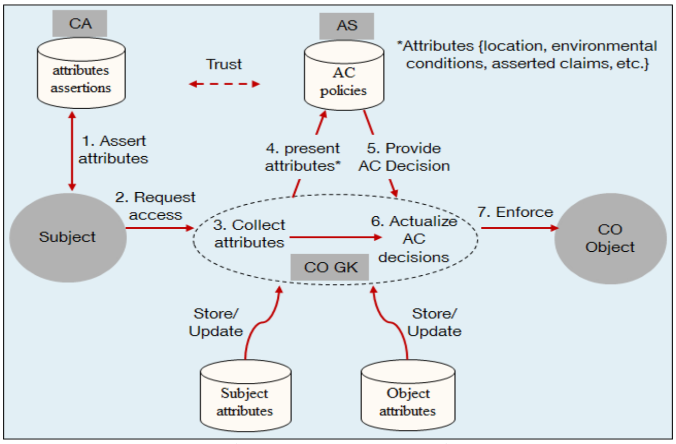

Fig.2. COBAC Framework

C. *Usability Scenario*

In order to demonstrate COBAC approach in real life setting we present a usability scenario, as shown in Fig. 3. In this scenario, IoT objects in a smart home is members of two two communities (COs). COβ includes smart objects which can accommodate inhabitants and guests in a smart home and COα which is rather private and its usage is reserved for the smart home inhabitants and selected other members. The AS is administered by the smart home owner or by the building manager; and there is a pre-established trust relationship between this AS and some pre-defined CAs. In which, the host at a smart home or the building manager can specify a list of CAs which the subjects can certify their attributes at. Examples of CAs are telecommunication companies i.e. via telephone number, location detection and maps services, social networks, etc. The GK role is assigned to smart objects with sufficient capabilities, including processing and storage capabilities, during the design time.

IV. Discussion

This paper proposes a candidate vision for administering AC in IoT namely community-based AC (COBAC). From an AC perspective, COBAC is proposed to meet the requirements which we presented as induced from literature. That is, envisioning an approach where authorization responsibility is split between a centralized server and community-level gatekeepers can help achieve a thin client/thin server architecture. Also, delegating the role of CA to parties of trust to the AS helps in realizing an open AC architecture. Finally, COBAC relies on attributes rather than solely the identity to authenticate requesting subject. And thus having to rely on a hefty identity management infrastructure can be avoided.

From an architectural perspective, the concept of community is utilized as means to govern AC across communities of IoT objects sharing the same mission. Thus, in this article we build on the conceptualization of community to define the notion of access rights. That is, an entity holding a certain access right means it has to play the role of the entitled party towards an obliged party in a relationship defined by the system of norms of a given community. Thus a GK in a given community is then able to acknowledge access rights-claim to evaluate if this rights-claim conforms to the set of policies of the community.

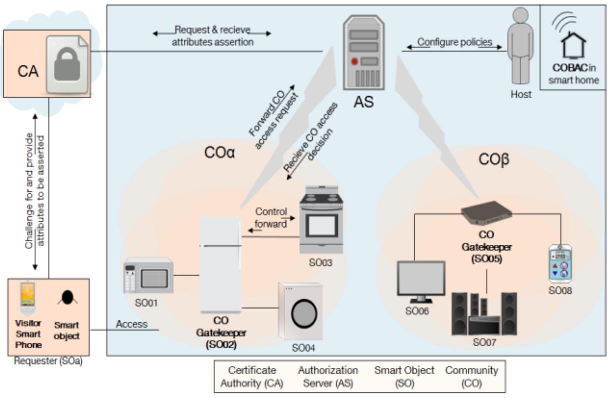

Fig.3. COBAC Usability scenario

This conceptualization of community can be adapted to realize AC in several use cases where it should be enforced within the boundaries of a community, as confidence and trust are expected in scenarios like:

- Home automation, where communities exist by default among connected objects with various resource capabilities and sharing common attributes in a smart home. These attributes include common missions (i.e. entertainment, household appliances, etc.) or privacy settings (i.e. private, public devices, etc.) or configuration steps and so on.
- Smart health monitoring, where communities can be established among patients' wearable devices that monitor vital signs and send it to an assigned physician or cloud-based repository for analyzing these data.
- Industry 4.0, where devices by default perform common functions and share common mission statement within a smart factory. In addition, devices provided by the same manufacturer and or uses the same technology to perform their intended tasks could be grouped in a community.

References

[1] S. Gusmeroli, S. Piccione, & D. Rotondi, (2013). A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling, 58(5), 1189-1205.

[2] V. G. Cerf , (2015).Access Control and the Internet of Things". IEEE Internet Computing, 19(5): 96.

[3] E. Kovacs (2016). Hosting Provider OVH Hit by 1 Tbps DDoS Attack. September 23, 2016. Retrieved from: http://www.securityweek.com/ hosting-provider-ovh-hit-1-tbps-ddos-attack. Accessed 8 February 2016.

[4] R. Dillet (2017). Netatmo is trying really hard to make the smart home happen. January 3, 2017. Retrieved from: https://techcrunch.com/2017 /01/03/netatmo-is-trying-really-hard-to-make-the-smart-home-happen. Accessed 8 February 20 16.

[5] B. Anggorojati, P. N. Mahalle, N. R. Prasad, & R. Prasad, (2012). Capability-based access control delegation model on the federated IoT network. In Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on (pp. 604-608). IEEE.

View publication stats