Poster: Activity-Based Access Control for IoT

Lyes Touati, Yacine Challal

Poster: Activity-Based Access Control for IoT

Lyes Touati
Sorbonne universités, Université de technologie de Compiègne,
CNRS, Heudiasyc UMR 7253,
CS 60 319, 60 203 Compiègne cedex.
lyes.touati@utc.fr

Yacine Challal
Ecole nationale Supérieure d'Informatique,
LMCS, CERIST.
Algiers, Algeria
y_challal@esi.dz

ABSTRACT

In traditional access control systems, a process is granted or not the access to a resource following a control on a single action without taking into consideration user and/or system context. In this paper we introduce a novel concept and a generalized version of context-aware access control in the Internet of Things that we name *Activity Control*. Our approach is aimed to be aware of the user's context and the overall system's one to make decision on granting or denying the requested action. To implement our concept we used a finite-state machine and the asymmetric encryption mechanism called Ciphertext-Policy Attribute-Based Encryption to achieve a real-time access policy adaptation following user's and/or system's context evolution.

Categories and Subject Descriptors

D.4.6 [**OPERATING SYSTEMS**]: Security and Protection—*Access controls*

Keywords

Internet of Things, Activity Control, Access Control, CP-ABE, Finite-State Machine

1. INTRODUCTION

Internet of Things (IoT) is an enabling technology for Cyber-Physical Systems or Systems of Systems. Indeed, Internet is evolving from a network of personal computers and servers toward a huge network interconnecting billions of smart communicating objects. These objects will be integrated into complex systems and use sensors and actuators to observe and interact with their physical environment, and hence allowing interaction among autonomous systems.

IoT will be involved in various applications ranging from military (enemy territories exploration, soldiers monitoring, ...), to e-health (monitoring elder-lies, remote diagnosis, ...), smart cities, smart grid, smart vehicles and transportation (traffic jam management), etc. Given the sensitivity of IoT applications, access control becomes a compulsory security service to prevent attacks against those sensitive applications that would have a deep impact and great damages on the systems themselves and their users and customers. Privacy is another issue that requires fine-grained access control to avoid access to private information by third parties. However, what should be protected from disclosure depends heavily on user's and/or system's context. Moreover, the access policy may evolve following a change in the user's context. What must remain confidential under some circumstances, may be a vital input for a third party for user's safety and security. For instance, a person may deny access to her/his location to preserve her/his privacy. If it comes that the same person falls in a isolated location and needs help, activation to her/his location may be vital. Therefore, access control policy must be adaptive and context-aware. In this paper, we introduce a new concept in IoT security that we call *Activity Control*, it allows a fine-grained and context-aware access control that takes into consideration user's context evolution.

In the remainder of the paper, we present related works in section 2. Section 3 presents our motivations, the principle of our approach and how we intend to implement it. Then, we conclude in section 4.

SmartObjects'15, September 07-11 2015, Paris, France.
ACM 978-1-4503-3535-5/15/09.
http://dx.doi.org/10.1145/2797044.2797052.

2. RELATED WORKS

In the literature, there are many access control systems that are applied to IoT. Access control solutions in IoT are divided mainly into Three approaches: Role based access control [1], Trust based access control [2], and Credential based Access Control. In the latter category, solutions require a user to have some credentials to gain access to some resource or data, we can cite two subcategories:

Attribute-Based: a user must have some attributes to be able to access a resource. Giuseppe Bianchi et al. proposed AGREE [3]: an Access control for GREEn wireless sensor networks, which implements the multi-authority version of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4] in energy harvesting wireless sensor network.

Capability-Based: A capability (known in some systems as a "key") is communicable, unforgeable token of authority, it refers to a value that uniquely references an object along with an associated set of access rights. The capability token grants a process the capability to interact with an object in certain ways. IACAC [5], CCAAC [6] and CapBAC [7] are some examples of capability based solutions of access control in IoT.

All these access control solutions are limited when applied to IoT applications, this is because they are not context aware and are unable to control objects' activities.

3. ACTIVITY CONTROL

3.1 Principle

The idea of our approach is to use a finite-state machine to model objects' states. Each object has an associated specific finite-state machine that is built during system design phase and stored by the Attribute Authority. The finite-sate machine contains all states of an object during the life of the system, it specifies also when and/or how an object passes from one state to another, this is what we call a *trigger*. Each state of the finite-state machine is associated with a list of object privileges, and each transition/arrow is labeled by a list of triggers as shown in figure 1-a. A privilege is the ability to execute an action over a resource, access to a data, ... etc. A trigger is an event that causes the change of state of an object which reflects the change in object's privileges. It can be a fixed time, an event occurred in object's environment, an action of the object itself over another object ... etc.

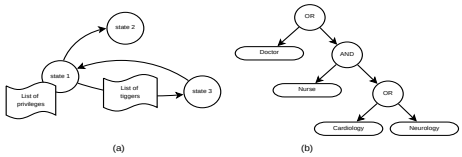

Figure 1: (a) Finite-State Machine; (b) Access Tree

3.2 Implementation

To implement activity control we propose to use CP-ABE [4]. The list of privileges associated to each state is materialized by an attributes list from which a secret key is generated by the Attribute Authority. The secret key determines which action is authorized and which one is not.

The object transition from a state to another induces the loss and/or acquisition of some attributes/privileges. This could be achieved by developing a real-time attribute revocation mechanism for CP-ABE.

Objects can offer some services to other objects. Each service is associated with an access policy defined by an access tree. Figure 1-b shows an example of access tree which can be rewritten this way: (*"Doctor"* **OR** (*"Nurse"* **AND** (*"Cardiology"* **OR** *"Neurology"*))). The access policy determines who is authorized to access the service without giving information about receivers identities. When an object solicits a service from another object, the latter verifies if the requester secret key satisfies the access policy defined for the requested service.

3.3 Work in progress

It is well-known that the attribute revocation is a tricky problem in Attribute-Based Encryption (ABE). This is because the party encrypting the data is not able to distinguish the revoked parties from others. The solution named Piratte [8] seems to be suitable in our case. However, it is able to revoke only up to a predefined numbers of users/attributes. In a first step, we can use it to implement our activity-based access control. In a second step, we plan to develop of a novel real-time attribute revocation mechanism without re-encryption for CP-ABE. The idea of our solution is to generate a secret key for every state of an object. These secret keys will be sent partly to the corresponding object. An object will able to decrypt ciphertexts in real-time even if it does not have the complete secret key. As soon as an object transits from a state to another, its current secret key will be useless and another one is generated based on the privileges list corresponding to the new state. This new secret key is also sent partly and replaces the old one. Our solution is intended to offer an efficient immediate attribute/user revocation for CP-ABE.

4. CONCLUSION

In this paper we introduced the concept of Activity Control in the Internet of Things as generalization of Access Control while taking into consideration the context of objects and the system. We used a finite-state machine combined to CP-ABE to implement our concept.

As future work, we plan to develop an efficient and real-time attribute revocation mechanism for CP-ABE.

5. ACKNOWLEDGMENT

This work was carried out and funded in the framework of the Labex MS2T. It was supported by the French Government, through the program "Investments for the future" managed by the National Agency for Research (Reference ANR-11-IDEX-0004-02).

6. REFERENCES

[1] J. Liu, Y. Xiao, and C. P. Chen, "Internet of things' authentication and access control," *Int. J. Secur. Netw.*, vol. 7, no. 4, pp. 228–241, 2012.

[2] P. Mahalle, P. Thakre, N. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in internet of things," in *VITAE*, 2013, pp. 1–5.

[3] G. Bianchi, A. T. Capossele, C. Petrioli, and D. Spenza, "Agree: exploiting energy harvesting to support data-centric access control in {WSNs}," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2625 – 2636, 2013.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2007.

[5] N. R. P. Parikshit N. Mahalle, Bayu Anggorojati and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309–348, 2013.

[6] B. Anggorojati, P. Mahalle, N. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated iot network," in *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*, Sept 2012, pp. 604–608.

[7] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," *Mathematical and Computer Modelling*, vol. 58, no. 5-6, 2013.

[8] S. Jahid and N. Borisov, "Piratte: Proxy-based immediate revocation of attribute-based encryption," *arXiv preprint arXiv:1208.4877*, 2012.