Authorization specification and management in cloud infrastructures

13 septembre 2024

Keywords : , distributed security policies, access control
Contact :
Clara Bertolissi, {clara.bertolissi}@lis-lab.fr
Laboratoire d'Informatique et Systèmes, LIS, UMR 7020, Luminy, Marseille, France (http://www.lis-lab.fr)

Objectives : The final objective of this thesis is to develop a formal framework for authorization specification and management in cloud infrastructures, as well as the development of abuse of privileges detection mechanisms via a learning-based approach.

Context : In this thesis we focus on authorization management models and mechanisms in Cloud environments. An authorization system must satisfy the key security properties of confidentiality (preventing unauthorized disclosure of resources), integrity (preventing modification of resources without authorization), and availability (ensuring access to a resource by legitimate users when necessary). Cloud-Edge environments are characterized by limited trust, variable computing power, and the involvement of multiple actors with different goals, which complicates the enforcement of security and privacy policies. There is a need of security mechanisms that ensure control over data and its uses.

This thesis aims to develop a scalable authorization framework for Cloud applications. Also, abusive access detection will be used to both dynamically limit unauthorized information disclosure and allow access control policies refinement in order to make the principle of least privilege effective.

Part 1 : *Access control models and mechanisms.*

Models that rely on user identities are not fully suited to decentralized and distributed systems. Our goal is to provide a formal access control framework to specify operations and decision-making procedures in a distributed and federated cloud system [GMGC23]. We will propose a high-level specification of access policies in order to manage the complexity introduced by the cooperation

of different applications with the environment and the users. The proposed model will be inspired by attribute-based access control and support the notions of contextual information, user groups and relationships between entities (causal, social, defined by the application, etc.)[HW20]. The model we aim to develop will provide a more fine-grained control w.r.t. traditional models. In particular, different users may have different relationships with the same resources, and resources (or applications) may have dependencies between them. Furthermore, we aim to support controlled sharing through collaborative decision-making. The application of authorization mechanisms is closely linked to their definition language and their execution at multiple points of the system, in a centralized, distributed or hybrid manner. Nowadays, most of the existing solutions rely on a centralized authorization module, which can include policy administration and credential management for authorization decisions (e.g., the authorization server in the case of OAuth2.0 or the PDP/PEP module in the case of XACML). A Cloud-based IAM solution will be proposed as a service, using a "SaaS" (security as a service) approach.

Part 2 : *Privilege Abuse and Mitigation Measures.*

The level of security offered by an access control system mainly depends on the correctness of the access control policies used. To this end, several principles to guide the specification of access control policies have been proposed (least privilege, separation of duties, etc.). However, once access privileges are assigned to a user, there is no guarantee that the user will not misuse them. We want to study a proactive solution to detect privilege abuse by complementing the access control system with an anomaly detection system. We would like to exploit learning approaches for the detection of abnormal user behaviors, in order to learn the behavioral profiles of users accessing resources and to accurately refine the policies [MNN23]. There may be different behavioral profiles, to be determined based on the analysis of contextual knowledge concerning users and resources. Such knowledge has proven to be a valuable source of information for approaches dedicated to improving the detection of internal threats to systems and access control. In particular, the anomaly detection system must check whether access requests are abnormal according to the requester's access behavior profile and, in this case, react by triggering an alert indicating a possible misuse of privileges.

This thesis is part of the France2030 national project "TrustInClouds" funded by the French National Research Agency under the reference "23-PECL-0009". During his thesis, the doctoral student will be required to participate in working groups, summer schools and other activities supported by the project.

Références

[GMGC23] Lewis Golightly, Paolo Modesti, Rémi Garcia, and Victor Chang. Securing distributed systems : A survey on access control techniques

for cloud, blockchain, iot and sdn. *Cyber Security and Applications*, 1 :100015, 2023.

[HW20] Yanchun Zhang Hua Wang, Jinli Cao. *Access Control Management in Cloud Environments*. Springer Cham, 2020.

[MNN23] Lopamudra Praharaj Mahmoud Abdelsalam Ram Krishnan Ravi Sandhu Mohammad Nur Nobi, Maanak Gupta. Machine learning in access control : A taxonomy and survey. Technical report, arXiv :2207.01739, 2023.