Sujet de thèse

Solutions d'autorisation pour les environnements cloud

Laboratoire : Equipe Modelisation et Verification, Laboratoire d'Informatique et des Systèmes, Luminy, `http://www.lis-lab.fr`

Contact :
Clara Bertolissi Email : `{clara.bertolissi}@lis-lab.fr`

Contexte

Dans cette thèse nous nous concentrons sur les modèles et mécanismes de gestion des autorisations dans les environnements de type Cloud. Un système d'autorisation doit satisfaire aux principales propriétés de sécurité que sont la confidentialité (empêcher la divulgation non autorisée des ressources), l'intégrité (empêcher la modification des ressources sans autorisation) et la disponibilité (assurer l'accès à une ressource par des utilisateurs légitimes en cas de besoin). Les environnements Cloud-Edge se caractérisent par une confiance limitée, une puissance de calcul variable et l'implication de plusieurs acteurs ayant des objectifs différents, ce qui complique l'application des politiques de sécurité et de confidentialité.

La thèse sera constitué de deux parties, l'une sur un cadre formel de spécification des autorisations, l'autre sur la détection des abus de privilèges via une approche basée sur l'apprentissage.

Partie 1 : *Modèles et mécanismes de contrôle d'accès.*

Les modèles qui reposent sur les identités des utilisateurs ne sont pas totalement adaptés aux systèmes décentralisés et distribués. Notre objectif est de fournir un cadre formel de contrôle d'accès pour spécifier les opérations et les procédures de prise de décision dans un système distribuée et fédérée du type Cloud [GMGC23]. On proposera une spécification dynamique de haut niveau des droits d'accès pour gérer la complexité accrue qu'introduit la coopération entre différents applications, l'environnement et les utilisateurs. Le modèle proposé s'inspirera du contrôle d'accès basé sur les attributs et supportera les notions d'informations contextuelles, de groupes d'utilisateurs et de relations entre entités (causales, sociales, définies par l'application,...). Le modèle que nous visons à développer fournira un contrôle plus fin par rapport aux les environnements mono-utilisateur traditionnels. En particulier, différents utilisateurs peuvent avoir des relations différentes avec les mêmes ressources, et les ressources (ou applications) peuvent avoir des dépendances entre elles. Aussi, le modèle devra pouvoir intégrer des mécanismes de prise de décision collaborative. Les conflits d'accès seront traités et résolus de sorte à préserver au mieux les preferences de confidentialités des différentes parties prenantes [SRZ18].

Partie 2 : *Abus de privilèges et mesures de mitigation.*

Le niveau de sécurité offert par un système de contrôle d'accès dépend principalement de l'exactitude des politiques de contrôle d'accès employées. À cette fin, plusieurs principes pour guider la spécification des politiques de contrôle d'accès ont été proposés (moindre privilège, séparation des tâches, etc). Cependant, une fois les privilèges d'accès attribués à un utilisateur, il n'y a aucune garantie que l'utilisateur ne les utilisera pas à mauvais escient. Nous voulons étudier une solution proactive pour détecter les abus de privilèges en complémentant le système de contrôle d'accès avec un système de détection d'anomalies. On voudrait exploiter des approches d'apprentissage pour la détection des comportements anormaux des utilisateurs, afin d'apprendre les profils comportementaux des utilisateurs accédant aux resources et d'affiner avec précision les politiques [MNN23]. Il peut exister différents profils comportementaux, à déterminer sur la base de l'analyse de connaissance contextuelle qui concerne les utilisateurs et les ressources. Une telle connaissance a prouvé être une source précieuse d'informations pour les approches consacrées à l'amélioration de la détection des menaces internes aux système et du contrôle d'accès. En particulier, le système de détection d'anomalies doit vérifier si les demandes d'accès sont anormales selon le profile de comportement d'accès du demandeur et, dans ce cas, réagis en déclenchant une alerte signalant une possible utilisation abusive des privilèges.

Cette thèse s'inscrit dans le projet national France2030 "TrustInClouds" autour de la sécurité du Cloud. Le doctorant sera amené au cours de sa thèse à participer à des groupes de travail, écoles d'été et autres initiatives portées par le projet.

Références

[GMGC23] Lewis Golightly, Paolo Modesti, R©mi 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.

[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.

[SRZ18] Anna Cinzia Squicciarini, Sarah Michele Rajtmajer, and Nicola Zannone. Multi-party access control : Requirements, state of the art and open challenges. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '18, page 49, New York, NY, USA, 2018. Association for Computing Machinery.