Projet TREMPLIN RECHERCHE 2025/2026

Investigateur principal/ Coordonnateur : Thierry Grandpierre, ESIEE LIGM UMR CNRS 8049

Titre du Projet : Etat de l'art et mise en œuvre de l'implémentation de la gestion des rôles RBAC (Role Based Access Control) pour le durcissement des postes

Description du Projet :

Dans le cadre du durcissement (hardening) des postes, la réduction de la surface d'attaque est primordiale mais aussi le contrôle d'accès au plus bas niveau dans les systèmes d'exploitation.

Si la sécurisation par le déploiement de règles de sécurité est suffisamment mûre et bien explorée (hardeningKitty, openscap, Lynis, voir LUNAR et Tiger pour de l'audit), il en est tout autre pour la gestion des rôles.

L'importance d'effectuer un contrôle d'accès basé sur les rôles n'est plus à démontrer pour gérer les droits dans les applications de haut niveau des entreprises (IAM). En revanche, sa transposition dans les noyaux des systèmes d'exploitation en est encore à ces balbutiements aujourd'hui. Il n'existe pas encore de consensus mais seulement quelques axes de recherche identifiés et leurs implémentations plus ou moins opensource (Grsecurity, RSBAC, SELinux par la NSA). Ce sujet devient également de plus en plus critique au niveau de la gestion des containers (Docker/Kubernetes)

Travail attendu :

L'objectif du projet, puis du stage, est donc de faire un état de l'art des technologies de gestion des rôles au niveau noyaux des systèmes d'exploitation et en particulier l'existence de patch pour noyaux linux. Puis d'identifier et valider une solution par une mise en œuvre sur un système classique existant (Debian..). Dans une troisième partie il s'agira de confronter cette implémentation avec celle d'un poste déjà sécurisé, en particulier dans une solution open source de type Gallus/Gallis proposée par Eternilab. L'utilisation des extensions de fichier Posix 1003.2 (XATTR) est également un axe de durcissement des rôles qui pourra être utilisé pour le couplage des technologies.

Partenaires : J.M. Lacroix, S. Leroy, Eternilab

Lieu : ESIEE PARIS, Champs/Marne et visites ou visio avec les partenaires

Références bibliographiques :

Aditya Sissodiya, Eric Chiquito, Ulf Bodin, Johan Kristiansson, "Formal Verification for Preventing Misconfigured Access Policies in Kubernetes Clusters", IEEE Access, vol.13,

pp.141798-141813, 2025.

S. Long and L. Yan, "RACAC: An Approach toward RBAC and ABAC Combining Access Control," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1609-1616, doi: 10.1109/ICCC47050.2019.9064301.
keywords: {Authorization;Complexity theory;Task analysis;Analytical models;Maintenance engineering;information security;access control;RBAC;ABAC;hybrid policy},

M. Li, Y. Ma, Z. Yin, A. Chai, M. Lian and C. Wang, "A Security Access Strategy for Sensitive Resource of Intelligent Production Line System with Dynamic Attribute Collaboration," 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020, pp. 2201-2206, doi: 10.1109/ICCC51575.2020.9345298.
keywords: {Access control;Process control;Production;Dynamic scheduling;Security;Reliability;Industrial Internet of Things;dynamic attributes;intelligent production lines;sensitive information;secure access},

Permanent protection of information systems with method of automated security and integrity control
Author: Maxim O. KalininAuthors Info & Claims SIN '10: Proceedings of the 3rd international conference on Security of information and networks Pages 118 - 123
https://doi.org/10.1145/1854099.1854125