IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

AVIS DE SOUTENANCE DE THESE

DOCTORAT BRETAGNE LOIRE MATHSTIC

Mme Farah DERNAÏKA

(Dpt SRCD – Laboratoire Lab-STICC)

Soutiendra publiquement ses travaux en vue de l'obtention du grade de

Docteur d'IMT Atlantique

Dans le cadre de la co-accréditation de thèse d'IMT Atlantique

Le mardi 13 octobre 2020 à 19h00 à IMT Atlantique (Campus de Rennes)

Visio-conférence

(dispositions exceptionnelles durant la crise sanitaire liée au Covid19)

A posteriori log analysis and security rules violation detection

Résumé :

Les modèles de contrôle d'accès traditionnels empêchent les violations de la politique de sécurité en bloquant toute action non autorisée. Cependant, dans des environnements sensibles, comme dans le domaine de la santé, de nombreuses situations imprévues peuvent se produire, imposant la nécessité d'avoir un accès immédiat aux ressources d'information sans risque de rejet. Il est donc nécessaire de déployer un modèle de contrôle d'accès plus flexible.

Le mode de contrôle d'accès a posteriori consiste à surveiller les actions des utilisateurs afin de détecter d'éventuelles violations de la politique de sécurité et d'appliquer des sanctions et/ou des réparations. Ce processus de surveillance est basé sur l'analyse des fichiers journaux, où toutes les preuves d'accès persistent. Il doit être également associé à une politique de sanctions dissuasive afin que les utilisateurs ne soient pas tentés de violer la politique de sécurité. Dans la littérature, ce type de contrôle de sécurité a été divisé en trois étapes qui sont : le traitement des logs, l'analyse des logs, et l'imputabilité.

Cette thèse, a pour but d'étudier une approche reposant sur un contrôle a posteriori permettant de détecter toute violation de la politique de sécurité. Les trois domaines de ce type de contrôle sont donc abordés et de nouvelles solutions sont apportées. Dans la première étape, un médiateur sémantique est utilisé pour extraire des informations pertinentes des fichiers journaux. Ensuite, de nouveaux aspects sont traités pour une analyse efficace des logs, comme l'enrichissement sémantique et la conformité temporelle de la politique. De plus, l'analyse n'est pas limitée à la détection des violations qui peuvent être causées par les utilisateurs réguliers, mais considère aussi les violations des administrateurs. Enfin, un mécanisme d'imputabilité est proposé pour dissuader les utilisateurs de commettre des violations et appliquer des modalités de sanctions.

Mots-clés : Contrôle d'accès ; Analyse des logs ; Vérification temporelle ; Violations ; Sanctions

Le jury est composé de :

- M. Frédéric CUPPENS	Professeur	Polytechnique Montréal
- Mme Nora CUPPENS	Professeur	Polytechnique Montréal
- M. Mohand-Said HACID	Professeur	Université Claude Bernard Lyon 1
- M. Romain LABORDE	Maître de conférences	Université Paul Sabatier
- M. Olivier RAYNAUD	Maître de conférences	Be-almerys
- M. Eric TOTEL	Directeur de recherche	IMT Atlantique
- M. Alban GABILLON	Professeur des universités	Université de la Polynésie française (UPF)
- M. Joaquin GARCIA-ALFARO	Professeur	Telecom Sud Paris