République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique

Projet de mémoire pour l'obtention du diplôme de

Post Graduation Spécialisée

Option

Sécurité Informatique

Thème

Conception et réalisation d'un gestionnaire normalisé de politiques de sécurité, application au système de contrôle d'accès obligatoire AppArmor.

Sujet proposé et encadré par:

Dr. Bouabid Mohamed Amine

Maître de Recherche Classe B, Division R&D Réseaux, CERIST

Réalisé par :

Mlle. Khellas Amira

Soutenue le 16/02/2016

Devant le jury composé de:

Mme. A. ELMAOUHAB	Directrice de la division R&D Réseaux	Présidente
Mme. F. CHEKAOUI	Attachée de Recherche	Examinatrice
Mme. H. LADOUR	Attachée de Recherche	Examinatrice

- 2015-

Remerciements

Je souhaite remercier dans un premier temps Mr. Mohamed El Amine BOUABID de m'avoir encadré, orienté, aidé et conseillé.

Je tiens à remercier également toute l'équipe du service formation au CERIST pour l'accueil chaleureux qu'on m'avait accordé.

Je remercie également mes très chers parents, qui ont toujours été là pour moi, je tiens à les remercier pour leur conseil, leur soutien et leur patience.

Mes remerciements les plus chaleureux vont à tous mes camarades et collèges pour leurs encouragements dans les moments difficiles.

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

A mes parents.

Résumé

A l'heure actuelle, la sécurité des systèmes d'exploitation est un sujet de préoccupation dans les entreprises puisque avec l'évolution exponentielle des réseaux interconnectés ces systèmes sont de plus en plus ciblés par les hackers qui exploitent leurs vulnérabilités afin de nuire à la sécurité des systèmes d'information. Pour remédier à cela, plusieurs approches et mécanismes ont été utilisés afin d'assurer leur sécurité, dont le contrôle d'accès qui représente un élément indispensable. Cependant gérer la sécurité de l'ensemble de ces systèmes se révèle une tache difficile face à la diversité qu'ils présentent, pour cette raison, la normalisation de la gestion de sécurité de ces systèmes est devenue un réel enjeu.

Dans le cadre de notre projet, nous nous intéressons à normaliser la gestion des politiques de sécurité d'un mécanisme de contrôle d'accès obligatoire déployé dans les systèmes d'exploitation de la famille Linux nommé AppArmor.

En se fondant sur le standard CIM/WBEM, nous proposons un système permettant d'exprimer les règles et propriétés qui définissent les politiques du contrôle d'accès AppArmor en langage CIM, il s'agit d'un pilote (ou Provider) qui permet de traduire les règles de politique AppArmor en objets CIM et vice-versa, que nous allons intégrer dans une solution qui implémente tous les composants de l'architecture WBEM. Cependant, pour atteindre notre objectif, nous nous sommes retrouvés dans l'obligation de développer une bibliothèque qui permet de gérer le module AppArmor afin qu'elle serve comme élément de base dans le développement de notre provider, par conséquent, notre contribution s'est avérée double.

Notre travail représente une contribution dans le domaine de la gestion des politiques de sécurité des systèmes, l'approche adoptée (CIM/WBEM) permet d'introduire une abstraction sur le mécanisme de contrôle d'accès AppArmor implémenté dans différents systèmes Linux et d'assurer une gestion distribuée homogène et indépendante des plateformes.

Abstract

At the present time, the security of operating systems is a subject of concern in the companies, because with the exponential development of interconnected networks these systems are increasingly targeted by hackers exploiting vulnerabilities in order to affect companies' the information system. To remedy this, several approaches and mechanisms were used to ensure their security with access control that represents an essential element. However, handle the safety of all of these systems is proving a difficult task given the diversity they present. For this reason standardizing the security management of these systems has become an urgent necessity.

As part of our project, we are interested in standardized management of security policies of a mandatory access control mechanism deployed on the operating systems of the Linux family named AppArmor.

Based on the standard CIM/WBEM, we propose a system allowing to express the rules and properties that define the policies of the AppArmor access control in CIM language, it is a provider for translating the rules AppArmor policy into CIM objects and inversely, that we will integrate a solution that implements all the components of the WBEM architecture. However, to achieve our goal, we found ourselves in the obligation to develop a library which makes it possible to manage the AppArmor module so that it serve like a base foundation in the development of our provider, consequently, our contribution proved to be double.

Our work represents a contribution in the field of the management of the security policies of the systems, the approach adopted (CIM/WBEM) allows the introduction of an abstraction on the AppArmor access control mechanism implemented in the various Linux systems to ensure consistent and independent management of distributed platforms.

Table des matières