

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

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 collègues pour leurs encouragements dans les moments difficiles.

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

À 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 tâche 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

INTRODUCTION	13
Contexte.....	14
Objectif du projet.....	14
Organisation du mémoire.....	15
1. SYSTEME DE CONTROLE D'ACCES.....	16
1.1.Introduction.....	17
1.2.Le contrôle d'accès.....	17
1.2.1. Le but et les principes de base du contrôle d'accès.....	17
1.3.Les phases d'élaboration d'un système de contrôle d'accès.....	17
1.3.1. Les politiques de sécurité.....	17
1.3.1.1. Langages de spécification de politique de sécurité.....	17
1.3.2. Les modèles théoriques de contrôle d'accès	21
1.3.2.1. Les contrôles d'accès discrétionnaires (DAC).....	21
1.3.2.2. Les contrôles d'accès obligatoires (MAC).....	23
1.3.2.3. Les contrôles d'accès basé sur le rôle (RBAC)	25
1.3.2.4. Les contrôles d'accès basé sur l'organisation (ORBAC)	26
1.3.3. Les mécanismes de sécurité.....	26
1.3.3.1. SELinux.....	27
1.3.3.2. AppArmor.....	28
1.4.Conclusion.....	28
2. POLITIQUES DE CONTROLE D'ACCES APPARMOR.....	29
2.1.Introduction	30
2.2.Linux Security Modules (LSM)	30
2.3.Le mécanisme de contrôle d'accès AppArmor.....	31
2.3.1. Les applications immunisées par AppArmor.....	31
2.3.2. Architecture générale AppArmor.....	32
2.3.3. Les concepts de base d'AppArmor.....	33
2.3.3.1. Posix.....	33
2.3.3.2. Chroot.....	33
2.3.3.3. Le confinement.....	33
2.3.3.4. Profil	34
2.3.3.5. Transition de domaine.....	36
2.3.4. AppArmor dans la pratique.....	36

2.3.4.1. Les modes d'AppArmor.....	36
2.3.4.2. Les politiques d'AppArmor.....	36
2.3.4.3. Les permissions d'accès.....	37
2.3.4.4. Les composants d'un profil AppArmor.....	39
2.3.4.5. Exemple de profil AppArmor.....	40
2.4. Conclusion.....	41
3. LA GESTION DES POLITIQUES AVEC CIM/WBEM.....	42
3.1. Introduction.....	43
3.2. Web-Based Enterprise Management (WBEM)	43
3.2.1. La structure interne de l'architecture WBEM.....	44
3.2.2. Le protocole XML/HTTP.....	45
3.3. Le modèle d'information commun.....	45
3.3.1. Le méta modèle CIM.....	45
3.3.2. Le format Managed Object Format (MOF).....	47
3.3.3. Le modèle de donnée CIM.....	47
3.3.3.1. Le modèle de base.....	48
3.3.3.2. Le modèle commun.....	48
3.3.3.3. Les extensions du modèle CIM.....	50
3.3.3.4. Les opérations CIM.....	50
3.4. Le contrôle d'accès et la gestion des politiques dans CIM.....	51
3.4.1. Le modèle de politique CIM(CIM_Policy).....	52
3.4.2. Les profils CIM.....	53
3.4.2.1. Le profil de politique CIM.....	53
3.4.2.2. Le profil de gestion des politiques de contrôle d'accès intégré	54
3.5. Conclusion.....	55
4. CONCEPTION DU SYSTEME REALISE	56
4.1. Introduction.....	57
4.2. Architecture du système de gestion.....	57
4.3. Modélisation des politiques AppArmor.....	58
4.3.1. Diagramme de classe.....	58
4.3.1.1. Définition des politiques AppArmor.....	58
4.3.1.2. Application des regles de politique AppArmor.....	59
4.3.1.3. Description du modèle d'application des règles de politique AppArmor.....	61
4.3.2. Diagramme d'objet.....	67
4.4. Conclusion.....	69

5. REALISATION DU GESTIONNAIRE DE POLITIQUE DE SECURITE.....	70
5.1.Introduction.....	71
5.2.Les choix techniques.....	71
5.3.Implémentation	71
5.3.1. Implémentation de la bibliothèque de gestion AppArmor.....	71
5.3.1.1. Description des méthodes de libArmor.so.....	73
5.3.2. Implémentation du provider.....	74
5.3.2.1.Le module ARM_AccessControlService_Provider.....	74
5.3.2.2.Le module ARM_PolicyActivationService_Provider.....	74
5.3.2.3.Le module ARM_PolicyRule_Provider.....	74
5.3.2.4.Le module ARM_Profile_Provider.....	75
5.3.2.5.Le module ARM_ProfileSetting_Provider.....	75
5.3.2.6.Le module ARM_AbstractionSetting_Provider.....	75
5.3.2.7.Le module ARM_CapabilityEntriesSetting_Provider.....	75
5.3.2.8.Le module ARM_PathEntriesSetting_Provider.....	75
5.3.2.9.Le module ARM_NetworkEntriesSetting_Provider.....	76
5.3.2.10.Le module ARM_Log_Provider.....	76
5.3.2.11.Le module ARM_ServiceAffectsElement.....	76
5.3.2.12.Le module ARM_AssociatedPolicyActivationService.....	76
5.3.2.13.Le module ARM_ElementSettingData.....	76
5.3.2.14.Le module ARM_PolicyRuleInProfile.....	76
5.3.2.15.Le module ARM_AbstractionInProfile_Provider.....	76
5.3.2.16.Le module ARM_PathEntriesInProfile.....	76
5.3.2.17.Le module ARM_CapabilityEntriesInProfile.....	76
5.3.2.18.Le module ARM_NetworkEntriesInProfile.....	77
5.4. Phases de développement d'un provider.....	77
5.4.1. Phase de définition des classes en format MOF.....	77
5.4.2. Phase de génération des classes en C++.....	78
5.4.3. Phase de génération des squelettes des providers.....	78
5.4.4. Phase d'implémentation des providers.....	79
5.4.5. Phase de génération du module.....	80
5.4.6. Phase de compilation des providers.....	80
5.4.7. Phase d'enregistrement du provider.....	80
5.5.Plan de tests.....	81
5.5.1. Modification des paramètres d'AppArmor.....	81

5.5.1.1.Activation/Désactivation d'AppArmor.....	81
5.5.2.Création d'un profil AppArmor.....	82
5.5.3.Modification des paramètres d'un profil AppArmor.....	84
5.5.3.1.Activation/Désactivation d'un profil AppArmor.....	84
5.5.3.2.Modification du mode d'un profil AppArmor.....	85
5.5.4.Ajout de règles dans un profil AppArmor.....	86
5.6.Conclusion.....	89
CONCLUSION GENERALE ET PERSPECTIVES.....	90