Une approche orientée attribut pour le contrôle d'accès basé sur la hiérarchie organisationnelle

Dongmo Sopjio Flore

Université de Dschang

May 12, 2022

Plan de notre travail

Contexte de notre travail

Historique

Avec le développement de l'informatique et d'Internet, les données sont de plus en plus stockées dans des serveurs distants afin de faciliter leur utilisation et de réduire les coûts du matériel nécessaire pour leur stockage. Cependant, avec internet, la sécurité des données n'est pas sans faille. Ainsi il est possible d'accéder de façon frauduleuse à des supports de stockage contenant des données venant de divers individus (personne ou entreprises).

Contexte de notre travail

attaque sur les données

- le ransomware, qui est un logiciel malveillant qui prend en otage des données personnelles. il chiffre ces données et demande ensuite une rançon à son propriétaire afin qu'il puisse accéder à ces données.
-l'hameçonnage ou phishing, est une technique utilisée par les fraudeur pour obtenir des renseignements personnelles dans le but de perpétrer une usurpation d'identité.

Contexte de notre travail

statistiques des attaques sur les données

- Le 14 avril 2020, les informations d'identification de plus de 500 000 comptes de visio-conférence Zoom ont été trouvées en vente sur le dark Web.
- Le 18 février 2021, le California Department of Motor Vehicles (DMV) a alerté les conducteurs californiens qu'ils avaient été victime d'une fuite de données après que son prestataire de gestion de facturation, Automatic Funds Transfer Services, ait subi une attaque de ransomware.

Contexte de notre travail

contrôle d'accès

Le contrôle d'accès est une technique de sécurité qui permet de déterminer les utilisateurs ou les programmes autorisées à accéder et/ou à modifier des données sécurisées dans le système.

Contexte de notre travail

politique et modèle de contrôle d'accès discrétionnaire (DAC)

- Principe: Les politiques de protection discrétionnaires régissent l'accès des utilisateurs à l'information sur la base de l'identité de l'utilisateur et des autorisations qui spécifient pour chaque utilisateur (ou groupe d'utilisateurs) et chaque objet du système, les modes d'accès que l'utilisateur est autorisé à effectuer sur l'objet
- Avantages:elles sont faciles à implémenter, offrent une grande flexibilité et sont intégrées dans la plupart des système d'exploitation et flexible
-Inconvénients: les politiques discrétionnaire ne font pas la différence entre un utilisateur et un sujet. un autre inconvénient de ces politiques est qu'elles souffrent d'un problème de perte de confidentialité. d'où la création des politiques obligatoires

Contexte de notre travail

politique et modèle de contrôle d'accès basé sur les rôles (MAC)

- Principe: Les politiques obligatoires régissent l'accès sur la base de la classification des sujets et des objets dans le système. il est associé à chaque sujet et à chaque objet du système un niveau de sécurité. Le niveau de sécurité associé à un objet reflète la sensibilité de l'information contenue dans l'objet. Le niveau de sécurité associé à un utilisateur, également appelé autorisation, reflète la confiance de l'utilisateur dans le fait de ne pas divulguer d'informations sensibles à des utilisateurs non autorisés à les voir.
- Avantages: elles permettent de faire la différence entre l'utilisateur et le sujet et sont utilisées dans les Systèmes d'exploitation tels que vista et LINUX. Elles offrent un niveau hautement sécurisé d'administration aux sources d'information.
-Inconvénients: Les politiques mandataires sont lentes à administrer et sont également rigides dans leur fonctionnement. elles ne sont pas adaptées aux entreprises de grande taille. d'où RBAC

Contexte de notre travail

politique et modèle de contrôle d'accès obligatoire (RBAC)

- Principe: Les politiques basées sur les rôles régulent l'accès des utilisateurs aux informations sur la base des activités qu'ils exécutent dans le système. Ces politiques nécessitent l'identification des rôles dans le système. Un rôle peut être défini comme un ensemble d'actions et de responsabilités associées à une activité professionnelle particulière.
- Avantages: elles sont adaptées pour les entreprises avec un niveau de turn over élevé, elles respectent le principe de moindre privilège et facilitent la gestion des autorisation
-Inconvénients: vu que ces politiques n'accordent l'accès aux objets que sur la base des rôles, cela limite la flexibilité du contrôle d'accès.elles sont non adaptée à un contexte dynamique et distribué. Elles ne permettent pas l'expression des politiques contextuelles et ne permettent pas d'exprimer la structure d'une permission en fonction de l'application. c'est ainsi qu'Or-BAC a été proposer

Contexte de notre travail

politiques et modèles de contrôle d'accès basés sur les organisation (Or-BAC)

- Principe: Or-BAC est un modèle de contrôle d'accès basé sur les organisations. Il introduit un niveau d'abstraction permettant d'exprimer des politiques de contrôle d'accès indépendamment de leur implémentation.
- Avantages: elles offrent la possibilité d'exprimer les règles contextuelles relatives aux permissions, aux interdictions, aux obligations et aux recommandations.
-Inconvénients: elles ne permettent pas d'exprimer les règles spécifiques d'un super-utilisateur dans un SI. En d'autres termes, elles octroient tout le pouvoir au DBA (dataBase Administrator) d'une organisation en lui faisant une totale confiance.

Contexte de notre travail

politiques et modèles de contrôle d'accès basés sur les attributs (ABAC)

- Principe: ABAC est un modèle de contrôle d'accès dans lequel les requêtes d'un sujet pour effectuer des opération sur des objets sont accordée ou refusées sur la base d'attribut assignés du sujet, d'attributs assignés des objets, des conditions d'environnement et d'un ensemble de politiques spécifiées en fonction de ces attributs et conditions. Un attribut est une information élémentaire qui caractérise une sujet, un objet, une action ou une condition environnementale
- Avantages: ABAC Offre une plus grande flexibilité dans un environnement distribué, ouvert, partageable et dynamique où le nombre d'utilisateurs est très élevé. il permet un contrôle d'accès fin (modèle basé sur les attributs)
-Inconvénients: ABAC nécessite Fort besoin de provisioning et de maintenance des attributs. la gestion des permissions est difficile dans ABAC. dans des situations d'urgence, ABAC peut refusé l'accès à une utilisateur légitime suite à l'absence d'une valeur d'attribut lors d'une décision d'accès.

Contexte de notre travail

politiques et modèles de contrôle d'accès basés sur les rôles attribués)

- Principe: c'est un modèle issu de la combinaison de RBAC et d'ABAC. ce modèle accord les droits d'accès aux utilisateurs non seulement sur la base des rôles mais également des attributs.
- Avantages: Ce modèle introduit dans RBAC le notion de dynamisme grâce à la création automatique des permission et à l'attribution automatique des permissions aux rôles. Ce modèle facilite la gestion des permissions et permet la structuration des rôles
-Inconvénients: elles ne permettent pas d'exprimer les règles spécifiques au contrôle du super-utilisateur dans un SI

Contexte de notre travail

politiques et modèles de contrôle d'accès basés sur les rôles améliorés par les attributs (AERBAC)

- Principe: c'est un modèle issu de la combinaison de RBAC et d'ABAC. Ce modèle fournit un mécanisme de contrôle d'accès à grain fin qui non seulement prend en compte les informations contextuelles lors de la prise de décision de contrôle d'accès, mais convient également aux applications où l'accès aux ressources est contrôlé en exploitant le contenu des ressources dans la politique.
- Avantages: AERBAC conserve la flexibilité offerte par ABAC, tout en conservant les avantages de RBAC, à savoir une administration, une analyse des politiques et une révision des permissions plus facile.
-Inconvénients: Tout comme ses prédécesseurs, ce modèle octroie tout le pouvoir au DBA d'une organisation en lui faisant une totale confiance. Ce qui n'est pas très normal, car ce dernier, parfois, use de ce pouvoir pour faire du n'importe quoi avec le système.

Contexte de notre travail

politiques et modèles de contrôle basés sur la hiérarchie organisationnelle (HOr-BAC)

- Principe: HOr-BAC se base sur la structure organisationnelle d'une organisation afin de permettre la spécification des politiques de sécurité contextuelle relative aux permissions. Dans HOr-BAC, les permissions sont attribuées aux unités organisationnelles et les employés affectés à ces unités obtiennent les permissions qui les sont attribuées. Le modèle HOr-BAC implémente en son sein le concept de parapheur électronique. Il s'agit ici d'un processus de contrôle de l'émission et du traitement des requêtes dans un système d'information.
- Avantages: il permet le contrôle des opérations effectuées dans le SI par le super-utilisateur, d'exprimer les règles qui spécifient la hiérarchie entre les unités administratives et opérationnelles et d'empêcher l'ajout des entités virtuelles dans le système d'information d'une organisation
-Inconvénients: Dans HOr-BAC, les politiques de contrôle ne peuvent être définies que sur la base de l'unité organisationnelle à laquelle appartient un employé, ce qui limite ainsi la flexibilité du contrôle d'accès. Par conséquent il ne permet que de définir des politiques de contrôle d'accès à gros grain, c'est-à-dire des politiques qui ne sont définies que sur la base des unités organisationnelles.

Problématique

Problématique

Le problème qui se pose est le suivant : comment réaliser l'approche orientée attribut du modèle HOr-BAC afin qu'il permette un contrôle d'accès fin et flexible ?

Objectifs

Objectif générale

L'objectif principal de notre travail est de proposer un modèle de contrôle d'accès permettant un contrôle d'accès à grain fin et flexible.

Objectifs Spécifiques

Comme objectifs secondaires, notre modèle devra :
- Permettre une prise de décision dynamique
- Être applicable aux données Cloud
- Obéir à la structure organisationnelle d'une organisation et aux relations hiérarchiques qui existe entre les différentes unités organisationnelles d'une entreprise.
- Permettre de surveiller les différentes opérations effectuées au sein d'un système d'information.

Solution

notre travail sera structuré comme suite:

- Dans une premier temps nous redéfinirons les concepts de base du modèle HOr-BAC
- Puis nous redéfinirons sa politique de sécurité - En fin nous redéfinirons le principe de fonctionnement du parapheur électronique qu'implémente HOr-BAC

Merci pour votre aimable attention!!!