Généralités sur les politiques de contrôle d'accès

La sécurité d'un système informatique a pour but la protection des ressources (incluant les données et les programmes) contre la révélation (confidentialité), la modification ou la destruction accidentelle ou malintentionnée (intégrité), tout en garantissant l'accès pour les utilisateurs légitimes (pas de déni de service).

Assurer une telle protection nécessite que tout accès au système et ses ressource soit contrôlé, et que seuls les accès autorisés puissent avoir lieu.

Pour assurer la sécurité, plusieurs techniques sont employées dont le contrôle d'accès, le chiffrement et la cryptographie.

Remarque

Dans le cadre de ce cours, nous nous intéressons au contrôle d'accès.

Le contrôle d'accès a pour but de ne permettre que les actions légitimes, c'est-à-dire à empêcher qu'un utilisateur puisse exécuter des opérations qui ne devraient pas lui être permises.

Pour définir quelles sont les opérations autorisées et celles qui sont interdites, il faut établir une politique de sécurité.

Définition

Le standard européen des ITSEC (Information Technology Security Evaluation Criteria) définit une politique de sécurité comme étant " l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique ".

Pour construire une politique de sécurité il faut :

- D'une part, définir un ensemble de propriétés de sécurité qui doivent être satisfaites par le système. Par exemple "une information confidentielle ne doit pas être transmise à un utilisateur non habilité à la connaître" ;
- D'autre part, établir un schéma d'autorisation, qui présente les règles permettant de modifier l'état de protection du système. Par exemple "le propriétaire d'une information peut accorder un droit d'accès pour cette information à n'importe quel utilisateur".

Si la politique d'autorisation est cohérente, alors il ne doit pas être possible, partant

d'un état initial sûr (c'est-à-dire satisfaisant les propriétés de sécurité), d'atteindre un état d'insécurité (c'est-à-dire un état où les propriétés de sécurité ne sont pas satisfaites) en appliquant le schéma d'autorisation.

Les axes de développement de la politique de sécurité

Une politique de sécurité peut se développer dans trois directions distinctes : les politiques de sécurité physique, administrative et logique.

1. La politique de sécurité physique précise un ensemble de procédures et de moyens qui protègent les locaux et les biens contre des risques majeurs (incendie, inondation, etc.) et contrôlent les accès physiques aux matériels informatiques et de communication (gardiens, codes, badges, ...).
2. La politique de sécurité administrative définit un ensemble de procédures et moyens qui traite de tout ce qui ressort de la sécurité d'un point de vue organisationnel au sein de l'entreprise. La structure de l'organigramme ainsi que la répartition des tâches (séparation des environnements de développement, d'industrialisation et de production des applicatifs) en font partie.
3. La politique de sécurité logique fait référence à la gestion du contrôle d'accès logique, lequel repose sur un triple service d'identification, d'authentification et d'autorisation. Elle spécifie qui a le droit d'accéder à quoi, et dans quelles circonstances. Ainsi, tout utilisateur, avant de se servir du système, devra décliner son identité (identification) et prouver qu'il est bien la personne qu'il prétend être (authentification). Une fois la relation établie, les actions légitimes que peut faire cet utilisateur sont déterminées par la politique d'autorisation.

A. Qu'est ce que le contrôle d'accès

Concrètement le contrôle d'accès consiste à gérer et à vérifier les droits d'accès, en fonction des règles spécifiées dans la politique de sécurité. On dit qu'un sujet (entité qui demande l'accès, dite aussi entité active) possède un droit d'accès sur un objet (entité à laquelle le sujet souhaite accéder, dite aussi entité passive) si et seulement s'il est autorisé à effectuer la fonction d'accès correspondante sur cet objet.

Complément

Les droits d'accès peuvent être symboliquement représentés dans une matrice de droits d'accès dont les lignes représentent les sujets et les colonnes représentent les objets. Une cellule de la matrice contient donc les droits d'accès d'un sujet sur un objet. La matrice est gérée conformément aux règles définies dans la politique de sécurité.

D'une manière générale, les règles de la politique de sécurité sont spécifiées en terme de :

- Permissions (par exemple tout médecin a le droit d'accéder aux dossiers médicaux de ses patients),
- Interdictions (par exemple, les médecins n'ont pas le droit d'effacer des diagnostics déjà établis),
- Obligations (les médecins sont obligés de conserver les dossiers médicaux pendant la durée fixée par la loi).

Définition

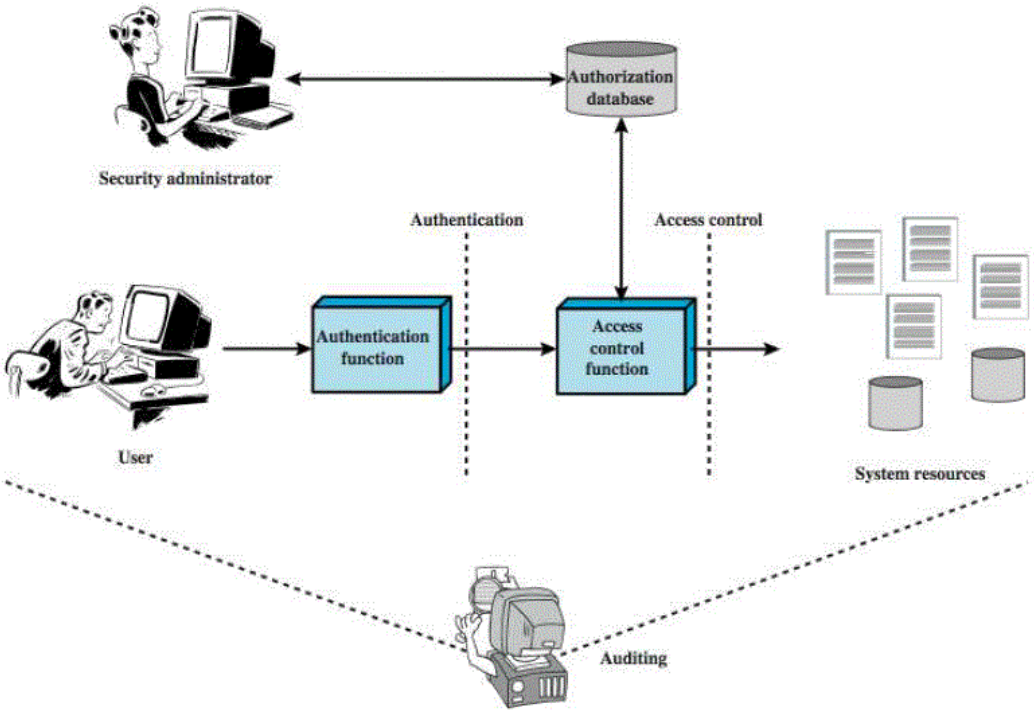
Le contrôle d'accès est un processus permettant de contrôler les tentatives d'accès afin de garantir les propriétés de sécurité suivantes : la confidentialité, l'intégrité et la disponibilité de service.

Rappel

- La confidentialité permet de protéger les ressources contre les révélations non autorisées,
- L'intégrité permet de prohiber les modifications non appropriées des données,
- La disponibilité de service permet de garantir l'accès aux informations et services.

Définition

Le contrôle d'accès est un mécanisme par lequel un système autorise ou interdit le droit à des entités actives (sujets : personnes, processus, machines, etc.) d'accéder et d'effectuer des opérations sur des entités passives (objets : fichier, dossier, etc).



Contrôle d'accès

B. Niveaux du contrôle d'accès

Le contrôle d'accès fonctionne à plusieurs niveaux :

- Logiciel
- Middleware

- Matériel

Niveau logiciel

Les mécanismes de contrôle d'accès au niveau des applications expriment des politiques de sécurité. Par exemple, dans une entreprise le personnel pourrait être affecté à plusieurs rôles différents. Chaque rôle peut initier plusieurs opérations possibles dans le système. Chaque opération nécessite des autorisations préalables pour pouvoir être exécutée.

Niveau middleware

Les applications peuvent être au dessus d'un « middleware », comme un système de gestion de base de données, qui met en application un certain nombre de propriétés de protection. Le middleware utilisera les moyens fournis par le système d'exploitation sous-jacent. Comme ce dernier construit les ressources de bas niveau telles que les fichiers et les ports de communication, il a donc la responsabilité de fournir les moyens de contrôler l'accès à celles-ci.

Niveau matériel

Les commandes d'accès de système d'exploitation se basent sur des fonctionnalités du matériel fournies par le processeur ou celle de la gestion de mémoire associée. Ces derniers contrôlent les accès d'un processus donné aux adresses de la mémoire.

C. Objectifs et propriétés du contrôle d'accès

Le contrôle d'accès est le moyen le plus utilisé pour sécuriser les systèmes et les réseaux informatiques. L'utilité du contrôle d'accès est d'assurer les propriétés de sécurité tel que :

1. La confidentialité
2. L'intégrité
3. La disponibilité

La confidentialité

Assurer que l'information ne soit accessible qu'à ceux qui ont l'autorisation.

L'intégrité

Assurer que l'information ne puisse être modifiée par des personnes non autorisées.

La disponibilité

Empêcher les données d'être supprimées ou de devenir inaccessibles. Cela s'applique non seulement aux informations mais aussi aux machines en réseau ou à d'autres aspects de l'infrastructure technologique.

Remarque

L'impossibilité d'accéder à des ressources requises est appelée un refus de service (Denial of Service).

Propriétés du contrôle d'accès

Le contrôle d'accès repose sur 3 propriétés importantes :

1. Authentification

2. Autorisation
3. Non-répudiation

Authentification

Assure que l'identité de l'utilisateur est légitime.

Autorisation

Détermine les tâches qu'un utilisateur est autorisé à faire.

Non répudiation

Assure qu'un utilisateur ne peut pas nier avoir effectué une tâche .

D. Les phases d'élaboration d'un système de contrôle d'accès

L'élaboration d'un système de contrôle d'accès s'effectue par une approche multi phases basée sur les concepts suivants :

1. Les politiques de sécurité
2. Les modèles de sécurité
3. Les mécanismes de sécurité

Les politiques de sécurité

Elles définissent les règles de haut niveau qui régissent les accès et décident lesquels sont autorisés pour garantir un système sûr.

Autrement dit, la politique de sécurité d'un système est l'ensemble des lois, des règles et des pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique.

Les modèles de sécurité

Ces modèles décrivent une représentation abstraite (souvent formelle) des politiques de sécurité et de leur fonctionnement.

Ils permettent de faciliter la construction de preuves sur la sécurité d'un système, c'est la raison pour laquelle les efforts se sont focalisés autour de la construction des modèles pour la sécurité.

Les mécanismes de sécurité

Ceux-ci définissent les fonctions de bas niveau (logiciels et matériels) permettant de mettre en application les contrôles imposés par la politique de sécurité.

Remarque

Les trois concepts précédents correspondent à une séparation conceptuelle entre différents niveaux d'abstraction de l'élaboration d'un système de contrôle d'accès, ce qui offre les avantages connus du développement multi-phases.

En particulier la séparation entre politiques et mécanismes, introduit une indépendance entre les besoins de protection à assurer et les techniques de mise en œuvre. Ainsi l'évolution des besoins ne remet pas en cause les techniques d'implémentation et inversement l'utilisation de nouvelles technique ne nécessite pas la reformulation des besoins.

Remarque

Le mécanisme de contrôle d'accès doit fonctionner comme un moniteur de référence qui est un composant sûr interceptant toute requête vers le système. Il doit présenter les propriétés suivantes :

- Inaltérable : il ne doit pas être possible de le modifier. Ou au moins que toute modification doit être détectable.
- Incontournable : Il interfère dans tout accès vers le système et ses ressources.
- Noyau de sécurité : Il doit être confiné dans une partie limitée du système pour simplifier sa vérification.
- Petite taille : La taille du module doit être limitée pour simplifier sa vérification.

E. Concepts de base

Le contrôle d'accès consiste à gérer et à vérifier les droits d'accès, en fonction des règles spécifiées dans la politique de sécurité. On dit qu'un sujet possède un droit d'accès sur un objet si et seulement s'il est autorisé à effectuer la fonction d'accès correspondante sur cet objet.

Sujets

Ce sont les entités actives du système qui :

- Demandent des droits d'accès correspondant à l'autorisation d'exécuter des actions sur les objets
- Incluent toujours les utilisateurs du système
- Incluent souvent les processus en cours d'exécution pour le compte des utilisateurs

Les objets

Ce sont les entités passives du système. Elles contiennent les informations et ressources à protéger.

Les actions

Ce sont les moyens permettant aux sujets de manipuler les objets du système

Principe du moindre privilège

Ce principe consiste à affecter des préférences aux utilisateurs de façon à ce qu'ils aient pas plus de permissions que nécessaires pour effectuer leurs tâches

L' application stricte de ce principe entraîne :

1. Différents niveaux de permissions
2. Différents niveaux de permissions à des moments différents
3. Permissions limitées dans le temps

Exemple : Domaine médical

- Sujets : médecins, infirmiers, secrétaire médicale
- Objets : patients, dossier médical ou administratif
- Actions : consulter, modifier le dossier médical d'un patient, créer le dossier médical d'un patient

Forme des règles d'une politique de sécurité

un sujet s a (la permission, l'interdiction, l'obligation) de réaliser l'action a sur l'objet ou l'ensemble des objets o.

Nous distinguons plusieurs types de règles :

- Règles indépendantes du contexte : accès à un objet ou un ensemble d'objets indépendamment du contexte.
- Règles dépendantes du contexte : accès aux objets à condition de vérifier le contexte donné.
- Règles de délégation et de transfert de droits : déléguer à un autre utilisateur la possibilité de réaliser certaines opérations ou un de ses droits d'accès.

Exemple

- Règles indépendantes du contexte :

  une secrétaire médicale a la permission de créer le dossier médical d'un patient.

  un patient a la permission de consulter son dossier.
- Règles dépendantes du contexte :

  un médecin qui est en grève a l'interdiction de consulter les dossiers médicaux de ses patients.
- Règles de délégation et de transfert de droits :

  un médecin a la permission d'autoriser un infirmier à consulter le dossier médical d'un patient.

F. Classification

Les politiques de sécurité, ou plus précisément leurs schémas d'autorisation, se classent en deux grandes catégories : les politiques discrétionnaires (ou DAC pour Discretionary Access Control) et les politiques obligatoires (ou MAC pour Mandatory Access Control).

Il existe également des variantes de ces politiques qui peuvent mieux s'adapter à des organisations particulières, comme politiques basées sur la notion de

- Rôles (ou RBAC pour Role-Based Access Control)
- Équipes (ou TMAC pour TeaM-based Access Control)
- Tâches (ou TBAC pour Task-Based Access Control)
- Organisation (ou ORBAC pour Organisation-Based Access Control)

Idéalement, il faut construire une politique de sécurité de telle sorte qu'aucune séquence valide d'applications des règles (du schéma d'autorisation) ne puisse amener le système dans un état tel qu'un objectif de sécurité soit violé, en partant d'un état initial sûr (on parle de politique de sécurité cohérente). Ceci suppose l'utilisation d'une méthode formelle de construction des règles du schéma d'autorisation, à partir d'une spécification formelle des objectifs de sécurité.

Les politiques d'autorisation les plus citées dans la littérature sont généralement associées à un modèle de sécurité. D'une manière générale, un modèle peut être défini comme un formalisme (souvent mathématique) qui offre une vue subjective mais pertinente de la réalité.

On modélise pour mieux comprendre le système qu'on développe, c'est-à-dire pour visualiser ses propriétés, spécifier sa structure ou son comportement, documenter et guider sa construction.

À partir de là, un modèle de sécurité peut être défini comme un formalisme permettant de représenter, de façon claire et non-ambiguë, la politique de sécurité.
Il aide à l'abstraire (afin de réduire sa complexité) et à faciliter sa compréhension, comme il peut servir à vérifier que cette politique est complète (tout est protégé) et cohérente, et que la mise en œuvre par le système de protection est conforme aux propriétés attendues du système.

Les modèles de sécurité peuvent être classés en deux grandes familles :

1. Des modèles généraux, qui sont plutôt des méthodes de description formelle, pouvant s'appliquer à toute sorte de politiques.
   C'est par exemple le cas de modèles de machines à états, représentant le système comme un ensemble d'états et de transitions qui, à partir d'un état courant et une valeur d'entrée, détermine le nouvel état du système.
   Il y a également les modèles basés sur les matrices d'accès, manipulant les trois concepts fondamentaux que sont les sujets, les objets et les actions. Les éléments qui se situent au croisement de la ligne L et de la colonne C correspondent aux droits possédés par le sujet correspondant à L sur l'objet de C ;
2. Des modèles spécifiques, développés pour représenter une politique d'autorisation particulière.
   Citons à titre d'exemple les modèles fondés sur les treillis, qui affectent à chaque utilisateur et à chaque objet un niveau de sécurité précis.