Cybersécurité - Cours 7: Contrôle d’accès et gestion des identités

SIO - Bloc 3 - SMDSI

M. SPINA

Sommaire

1) Introduction
2) Les risques
3) La gestion des accès
4) Exemple 1: RDVnet
5) Définitions
6) Exemple 2: Société nationale/internationale
7) Définitions (2)
8) Quelques métiers
9) Processus, outils et méthodes (4)

Introduction

Dans le monde professionnel, le recours aux technologies de l'information et des communications (TIC) semble indispensable de nos jours.

Cela est directement lié à l'évolution croissante des besoins des clients et de la production de données volumineuses.

Les risques

Information exposée → **vulnérabilité & risques potentiels**

Accès non autorisé: peut mettre en péril la disponibilité, l'intégrité ou la confidentialité de l'information qu'une organisation détient dans l'exercice de ses fonctions

→ causer des dommages importants, voire irréversibles, à l'organisation.

Altération ou destruction de données: peut engendrer des résultats inexacts ou incomplets, voire un ralentissement ou une interruption des services offerts. Exemple : altération avec intention de fraude.

Les risques

Divulgation de l'information ou vol de données: divers impacts

- atteinte à l'image de marque de l'organisation
- atteinte au droit des utilisateurs et à leur vie privée
- baisse de confiance des utilisateurs
- pertes financières, etc.

Augmentation du niveau de privilège: permet à une personne non autorisée d'accéder à de l'information sensible, voire de prendre le contrôle d'applications critiques pour l'organisation.
→ causer des dommages importants voire irréversibles

La gestion des accès

Mise en place de mesures de sécurité:

Gestion des droits et des privilèges d'accès:

→ permet à l'organisme d'assurer l'équilibre entre la protection de l'information qu'il détient et l'attribution des privilèges aux utilisateurs pour qu'ils puissent travailler efficacement.

Ce processus complexe intègre différentes règles, procédures et technologies. La gestion nécessite la **contribution de l'ensemble des entités** administratives de l'organisme.

La gestion des accès: principes

La gestion des accès est basée sur les **principes de privilège minimal** et de **séparation des tâches**.

Elle répond à 4 questions:

1) **Qui a accès à quelle information?**
2) **Qui a approuvé l'accès?**
3) **L'accès est-il adapté aux tâches à accomplir?**
4) **L'accès et les opérations correspondantes sont-ils correctement surveillés, consignés et enregistrés?**

Exemple 1: RDVNet (prise de rendez-vous)

Société SSII

propose une application

Interface Employeur (Médecins, artisans, etc.)

Interface Utilisateur (Patients, clients, etc.)

Exemple 1: RDVNet (prise de rendez-vous)

Société locale SSII

différents rôles sont attribués au sein de la société (Support, Communication, Dev, etc.)

propose une application

rôle “Employeur” attribué par la société

Interface Employeur (Médecins, artisans, etc.)

rôle “User” attribué par la société

Interface Utilisateur (Patients, clients, etc.)

Définitions

Contrôle d'accès ou gestion des accès: consiste à vérifier si une entité (personne ou organisation) qui demande l'accès à un objet (fichier, BDD, programme) possède les autorisations nécessaires.

Privilèges ou droits d'accès: désigne l'opération recherché à l'égard d'un objet (lire, écrire, modifier, supprimer, imprimer, créer, copier, transmettre).

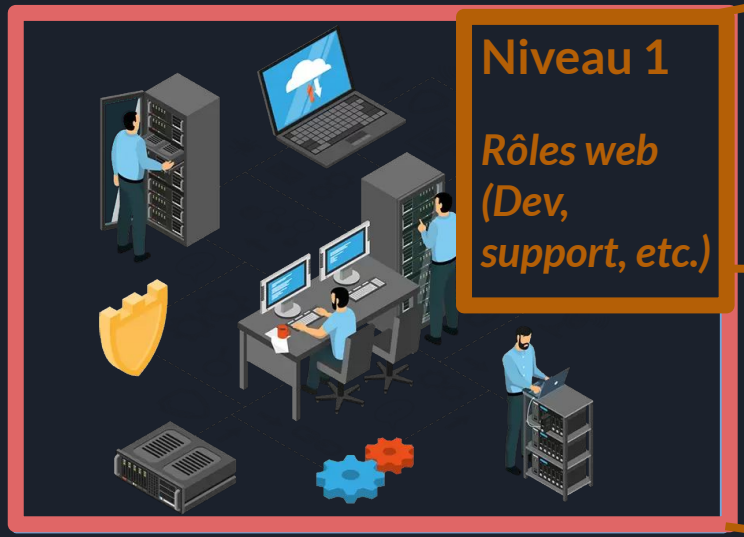
Rôle: définit l'ensemble des privilèges nécessaires à l'utilisation des objets (applications ou ressources).

Exemple 2: gestion du parc informatique

Société nationale/internationale

Niveau 0

Rôles locaux (RSI, DRH, prestataires, etc.)



Niveau 1

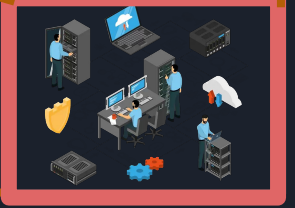
Rôles web (Dev, support, etc.)

Siège

Annexe A

Annexe B

Annexe C



Définitions

Rôle applicatif: définit l'ensemble de droits d'accès propres à une seule tâche dans une application.

Habilitation: regroupe plusieurs rôles ou rôles applicatifs permettant de hiérarchiser l'utilisation des ressources.

Matrice de profils d'accès général: grille associée à une entité contenant les rôles définis pour ses utilisateurs ou groupes d'utilisateurs.

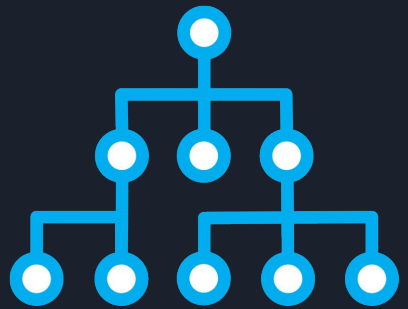
Matrice de profils d'accès applicatif: grille associée à un objet contenant les rôles applicatifs définis pour ses utilisateurs ou groupes d'utilisateurs.

Notions sur la gestion des ID et des accès

Les différents modèles

Beaucoup d'éléments ont été créés pour ou grâce à l'informatique et en fonction des domaines et des besoins diverses (langages, normes, réglementation, procédures, etc.)

La gestion des identités, elle, s'appuie sur des modèles existants, chaque modèle ayant une fonction particulière.



Le modèle IBAC (Identity-Based Access Control)

1971: premier modèle de contrôle d'accès

→ toujours utilisé par les OS (Windows) et les serveurs Linux

→ repose sur une **matrice** composée d'un **ensemble fini** d'entités, de ressources et de règles

→ établissement d'une **liste exhaustive** contenant les autorisations d'accès (**ACL: Access Control List**)

→ les habilitations sont **directement affectés aux comptes utilisateurs**

Le modèle IBAC: illustration

Ce modèle est le plus simple et reste adapté lorsque, dans le SI, le nombre d'utilisateurs et de ressources à protéger **est très faible**.

Utilisateurs	Répertoire /home	Fichier /etc/pwd	Ressource imprimante
Thomas	rw	rw	w
Maxime	rw	r	w

En effet, l'arrivée d'un nouvel utilisateur ou d'une nouvelle ressource **nécessite la mise à jour des habilitations**.

Le modèle MAC (Mandatory Access Control)

1973: contrôle d'accès obligatoire

→ fonctionne par **niveau de sécurité**

→ un niveau définit le niveau d'habilitation de l'utilisateur et de la ressource

→ l'utilisateur a accès à la ressource si son niveau d'habilitation est supérieur ou égal au niveau de classification de la ressource

Le modèle MAC: illustration

Dans cet exemple, les niveaux d'habilitations sont définis sur **3 niveaux**.

Utilisateurs	**Compte "Admin"**	**Compte "Gestionnaire"**	**Compte "Utilisateur"**
Habilitations	3	2	1

Ressources	**Application "Gestion des accès"**	**Application "Ciel compta"**	**Interface de connexion**
Habilitations	3	2	1

Le modèle MAC: évolution

1986: version étendue du modèle MAC

→ fonctionne toujours par niveau de sécurité mais **un intervalle de niveaux est attribué à toutes les ressources**

→ offre une plus **grande flexibilité**

→ modèle proche de celui utilisé actuellement par le **SGBD Oracle**

Exemple: un utilisateur peut accéder à toute information dont le niveau est compris entre la borne inférieure et la borne supérieure du niveau de l'utilisateur.

Le modèle RBAC (Rule-Based Access Control)

1992: modèle de contrôle d'accès par rôle

→ les habilitations sont **affectées à des rôles**

→ les rôles peuvent représenter des métiers, des activités, des projets ou des personnes physiques

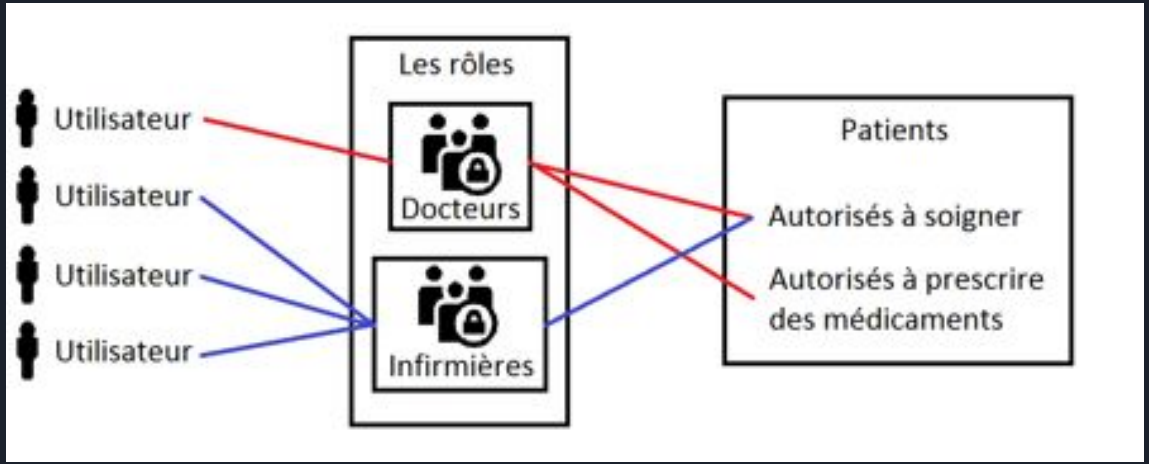
→ les rôles désignent le lien entre les utilisateurs et les ressources

→ il n'existe aucun modèle générique que l'on pourrait appliquer à différentes entreprises

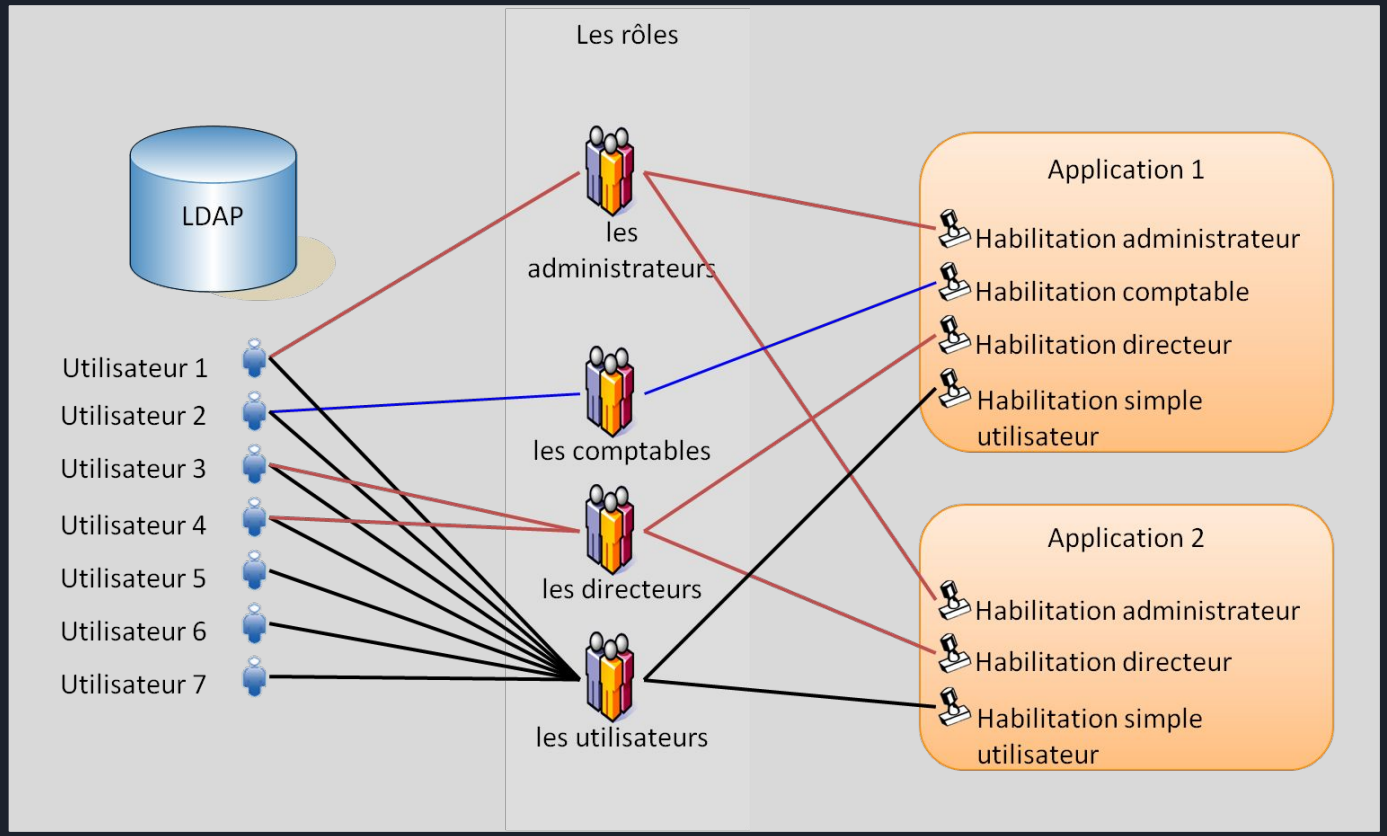
Le modèle RBAC: illustration

Toute modélisation RBAC demande une étude approfondie du SI.

Cet exemple minimaliste illustre les types d'habilitations affectés aux différents rôles au sein du secteur médical.



Le modèle RBAC: illustration 2



Le modèle RBAC: les limites

Le modèle RBAC **atteint rapidement ses limites** dès lors que les utilisateurs sont géographiquement différentiables, ou dès lors que l'entreprise est composée de services indépendants.

→ Par exemple, dans une société de services, les commerciaux sont attachés à des secteurs d'activités :

- un commercial chargé des affaires de l'industrie ne peut pas créer de contrat pour un client dans le secteur de la banque.

Le modèle RBAC: évolution

Pour pallier à ses limites, la notion de **groupe** apparaît en plus de celle de rôle ou de profil: **RBAC étendu**

→ association de profils ou de profils de profils aux utilisateurs

→ association de rôles ou de rôles de rôles aux applications

→ différencier les utilisateurs et les applications en fonction de critères tels que la géographie ou le secteur d'activité

Ce modèle est **suffisant pour la plupart des organismes** mais reste encore insuffisant pour de **grandes infrastructures** comme les hôpitaux.

Le modèle ORBAC (Organization-Based Access Control)

2003: modèle de contrôle d'accès fondé sur l'organisation

→ correspond à tout organisme nécessitant une grande logistique

→ reprend les concepts de rôle, d'activité, d'objets et d'organisation

https://fr.wikipedia.org/wiki/Contrôle_d%27accès_basé_sur_l%27organisation

http://irt.enseeiht.fr/anas/document/03Revue-InfoSyst.pdf

https://www.journaldunet.com/solutions/cloud-computing/1030351-l-insuffisance-du-modele-rbac/

Processus de contrôle des accès

Ce processus permet principalement de **créer, d'identifier, d'enregistrer** et **de gérer l'identité des utilisateurs et les droits d'accès** à l'information que détient l'organisme.

→ coordonner les tâches des différents intervenants afin de mettre en place les structures de contrôle nécessaires à la sécurité des accès

→ cela s'appuie sur le modèle RBAC

Quelques métiers

DRH: directeur des ressources humaines

COSI : conseiller organisationnel de la sécurité de l'information

COGI : coordonnateur organisationnel de gestion des incidents

ROSI : responsable organisationnel de la sécurité de l'information

Consultant IAM: expert en gestion des identités

Expert en sécurité informatique