La protection

G. Florin, S. Natkin
Novembre 2001

SCHÉMA D ’ACQUISITION ET D ’ÉVOLUTION DES DROITS

Quand un utilisateur se connecte sur son compte

- Il est authentifié
- il dispose alors de droits sur certains objets:
  - Les droits sur les objets systèmes que l ’administrateur lui donne.
  - Tous les droits sur les objets qu ’il crée.
  - Les droits sur d ’autres objets que les autres utilisateurs lui ont accordés.
  - Les droits de propagation des droits que l ’administrateur lui autorise
- Il peut créer de nouveaux objets et les droits correspondants
- Il peut propager des droits et donc donner des droits

C ’est la définition et le contrôle de ce schéma qui en théorie devrait garantir le respect des règles de sécurité.

LES TECHNIQUES DE LA SECURITE INFORMATIQUE

- Authentification des personnes
- Gestion des droits et contrôle d'accès (protection)
- Protocoles de sécurité
- Validation des systèmes

1- Spécification des politiques de contrôle d ’accès

GENERALITES

Le contrôle d ’accès est la base des mécanismes informatiques:
Il permet de spécifier la politique dans le domaine de l ’informatique.

Il définit la façon dont le système contrôle ces droits.

Il devrait, en théorie, encapsuler toutes les autres techniques informatiques
Pour l’instant ce n’est pas le cas.

CONCEPTS DE BASE

- Un ensemble de ressources physiques interconnectées et d'utilisateurs pour lequel est défini une politique de sécurité et est administré l'ensemble des règles et mécanismes de protection est appelé **cellule d'administration** (ce qui correspond dans l'environnement NT à la notion de domaine).
- A chaque utilisateur est associé un **compte**. Celui ci détermine les moyens qui doivent être utilisés pour authentifier cet utilisateur, les limite apportée au droit de connexion (les machines sur lesquelles il peut se connecter, le nombre maximal de connexions simultanées, les heures qui lui sont autorisées ou interdites…), et les droits initiaux qui lui sont accordés lors d'une connexion.
- Un **groupe** est un ensemble de droits communs à plusieurs utilisateurs. Par exemple sous NT à l'initialisation d'un domaine, le groupe administrateur à en particulier le droit de créer des groupes et des comptes ou de modifier la configuration physique du domaine de sécurité. Le groupe des invités a très peu de droits mais ses membres ne sont pas authentifiés.

EXEMPLES DE SPECIFICATION DE LA POLITIQUE

Un utilisateur a les droits de son compte (accès aux fichiers, programmes utilisables, ressources partagées accessibles)
Déterminée par une politique de compte.

Sous NT, les droits d'un utilisateur sont définis
les droits des groupes auquel il appartient (utilisateur de base + groupe des comptables).La gestion des comptes peut être très fine (par exemple on peut interdire au groupe des utilisateurs de base de se connecter la nuit)
Sous Unix (BSD), il y a trois groupes prédéterminés (moi, mon groupe, l'univers). Par contre on peut spécialiser individuellement les droits sur les ressources.

Sous 95,98 et Mac OS il n'y a rien de sérieux.

PRINCIPES A RESPECTER

Principe du **moindre privilège** : Un objet ne doit disposer que des droits qui lui sont strictement nécessaires pour réaliser les tâches
qui lui sont dévolues.

Utilisation de politique obligatoire : La politique doit le moins possible dépendre des utilisateurs en tant que personne,
mais reposer sur les rôles de la politique de sécurité du
système d’information.

Séparation des rôles de création des comptes et d ’attribution des droits

Les rôles d ’attribution des droits doivent être attribués par domaines de responsabilité

MATRICE DE CONTRÔLE D ’ACCES

Définit à chaque instant
les droits de chaque sujet sur chaque objet

	M1	M2	F1	F2	P1	P2
P1	**R,W,E**		**Own,R, W**	**R**		
P2		**R,W,E**		**Own,R, W**		
S1	**R,W,E, Create, Destroy**	**R,W,E, Create, Destroy**	**R,W,E, Create, Destroy**	**R,W,E, Create, Destroy**	**Create, Destroy**	**Create, Destroy**

MATRICE DE CONTRÔLE D ’ACCES (2)

A l'origine les types de sujet et d'objets sont prédéfinis (système)
sujets: utilisateurs, processus, groupes d'utilisateurs ou de processus
objets: segments ou pages mémoires, fichiers, processus, programmes

Ceci rend difficile la mise en oeuvre du principe du moindre privilège

Evolution vers une notion orientée objet
sujets: utilisateurs, objets
objets: métodes d'accès aux objets

	M1				
	R	**W**	**E**	**Create**	**Destroy**
P1	**1**	**1**	**1**		
P2					
S1	**1**	**1**	**1**	**1**	**1**

EVOLUTION DE LA MATRICE DE CONTRÔLE D ’ACCES

La matrice des droits évolue en fonction des évènements suivants:

- **création et destruction des sujets et des objets**
- **création et destruction des droits**
- **propagation des droits**

Exemple
Dans UNIX les droits d'un processus sont hérités de son père et donc originellement de l'utilisateur (fork du login)
Lorqu'un processus exécute un programme il hérite (SUID=vrai) en général des droits du possesseur du programme.

2-Authentification des personnes

AUTHENTIFICATION DES PERSONNES

L'**authentification** = **vérification de l'identité** d'une entité.

L'une des mesures les plus importantes de la sécurité:
- Impossible d'assurer la confidentialité, l'intégrité, la non répudiation sans la garantie de l'identité de l'entité soumettant une requête.
- L'authentification devrait être assurée en continu.
(pas une fois pour toutes à l'ouverture d'un objet (en début de session)
Personne **:**elle peut quitter son poste en le laissant ouvert
=> procédure de déconnexion automatique, procédure d'authentification périodique.
Entité informatique**:**une substitution peut avoir lieu
(surtout en réseau, nécessité de protocoles de sécurité)

L'authentification des personnes peut se faire par trois méthodes:
Ce que connaît l 'utilisateur (Mot de passe),
ce que détient l 'utilisateur (carte…),
ce qu 'est l 'utilisateur (Méthode biométrique)

CE QUE CONNAÎT L ’UTILISATEUR

Le mot de passe, le code confidentiel.Technique la plus simple et la plus répandue

Problèmes bien connus:

- Si le mot de passe est simple il peut être trouvé par une attaque par dictionnaire
- Si le mot de passe est compliqué l’utilisateur le note pour s’en souvenir !

Quelques parades:

- **Ne jamais utiliser** son login, son nom, le nom de son chien, son n°de tél., un mot d’un dictionnaire…Utiliser chiffres et lettres avec des caractères spéciaux au moins 6 à 7 caractères, mais trouver un mémotechnique
- **Obliger l'usager à changer** régulièrement de mot de passe.
- **Surveiller les tentatives d'accès** illicite par comptage (les afficher).
- **Prévenir l'usager des connexions** précédentes sur son compte en affichant la date et l'heure (par exemple du dernier accès).

CE QUE DETIENT L ’UTILISATEUR

Un secret matérialisé physiquement

La clé traditionnelle, la carte (magnétique, à code barre, à puce)

Technique simple, répandue.

Les problèmes :

- la perte, le vol du support
- la duplication (plus ou moins facile mais toujours possible)

CE QU ’EST L ’UTILISATEUR

les méthodes bio métriques

Une solution en rapide développement, peut-être très efficace,souvent onéreuse, peut-être difficile à accepter dans certains cas par l'utilisateur

Nécessité d'études approfondies (analyse de la variabilité) du caractère utilisé

- à l'intérieur du groupe humain des usagers autorisés.
- ou dans une population quelconque

Incertitudes des techniques bio métriques

- La variabilité intra-individuelle.
- La variabilité inter-individuelle.

conduisant à deux types d'erreurs possibles:

- Le rejet à tort d'un individu autorisé
- L'acceptation à tort d'une personne non autorisée.

QUELQUES TECHNIQUES BIOMÉTRIQUES À L'ÉTUDE

- L'empreinte digitale
- La vascularisation de la rétine
- La voix
- La géométrie de la main
- Dynamique de la signature
- Dynamique de la frappe clavier
- Empreinte génétique

3 Architecture des systèmes de protection

IMPLANTATION DE LA MATRICE DE CONTRÔLE D'ACCÈS: SYSTÈMES À CAPACITÉS

On appelle liste de **capacités (Capability)** une structure décrivant pour chaque objet O’ la liste des méthodes M_O de O que O’ peut exécuter.

Ceci revient à stocker les droits dans l’environnement de l’objet O qui demande l’opération et donc à stoker la matrice de protection en ligne.

IMPLANTATION DE LA MATRICE DE CONTRÔLE D'ACCÈS: LISTES DE CONTRÔLE D ’ACCÈS

On appelle **liste de contrôle d’accès** (**ACL : Access Control List**) associées à un objet O, une structure décrivant pour chaque objet O’ la liste des méthodes M_O de O que O’ peut exécuter.

Ceci revient à stocker les droits dans l’environnement de l’objet O qui exécute l’opération demandée et donc à stoker la matrice de protection en colonne.

COMPARAISON DES STRATEGIES (1)

Les listes de contrôle vision "centralisée" : ce sont les objets considérés comme serveurs de méthodes qui connaissent les objets client habilités à demander l'exécution d'une méthode.

- Pour créer, modifier ou révoquer un droit il suffit de s'adresser à ce serveur.
- Le serveur doit connaître tous les clients potentiels et tout processus de propagation d'un droit passe par le serveur .

COMPARAISON DES STRATEGIES (2)

Les capacités stockent les droits dans l'environnement des objets appelant une méthode (clients). Un tel objet montre au serveur, lors d'une demande de service, qu'il possède une capacité à faire cette demande.

- Version facilitant la répartition: laisse à chaque objet une capacité de créer et gérer ses droits.
- La révocation d'un droit est une opération complexe, puisqu'il faut à priori invalider le droit dans l'environnement de tous les objets qui le détiennent.

NOTION DE TICKET (PRIVILEGE, CLEF D'ACCES)

Un ticket est une structure qui représente à chaque instant les rôles que joue un objet dans le système.

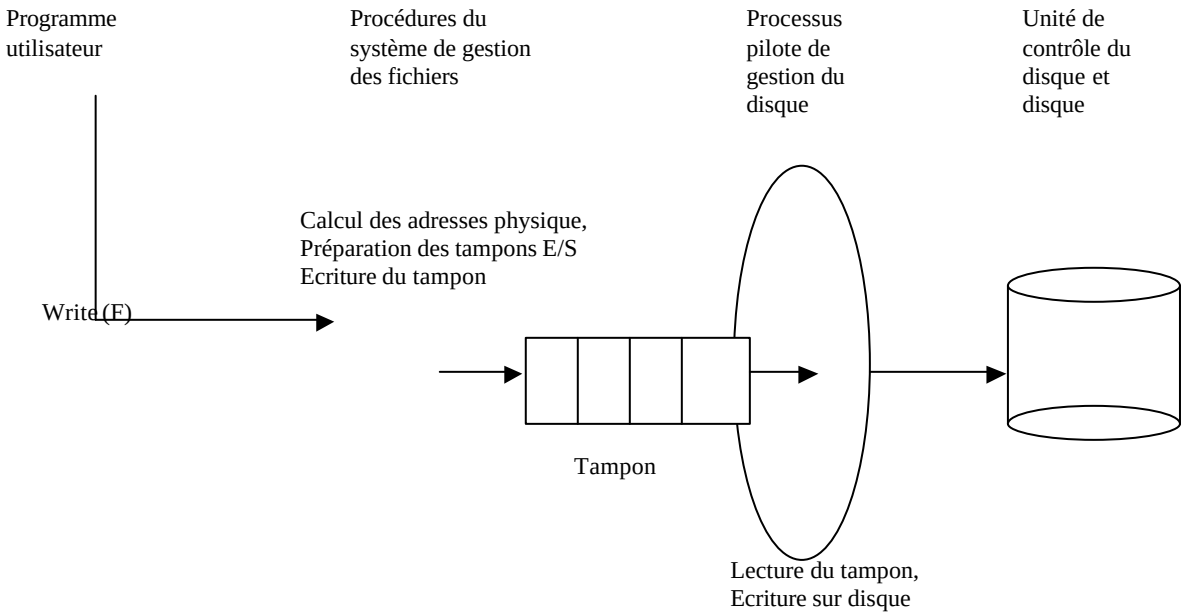
- Comme une capacité, un ticket est intègre et a une durée de vie limité. Il est stocké dans l'environnement de l'appelant.
- Ce n'est pas un droit.
- L'appelé qui, recevant un ticket, consulte une ACL liant les rôles et les droits d'accès. Ceci détermine si l'appelant à ou n'a pas un droit d'exécution.

HIERARCHIE DES MECANISMES DE PROTECTION
UN EXEMPLE (1)

Un utilisateur ouvre un fichier de texte sous un éditeur, procède à diverses modifications et écrit (opération enregistrer) une nouvelle version du fichier.

- L'utilisateur doit pouvoir éditer son fichier et donc lire et écrire sur le disque lorsque cela est nécessaire
- Il ne doit pas pouvoir lire ou écrire sur des fichiers qui ne lui sont pas accessibles et de façon plus générale accéder à toute zone du disque sans contrôle d'accès.
- Les mécanismes mis en place ne doivent pas pouvoir être contournés pour donner à un autre utilisateur non autorisé un accès un fichier F

HIERARCHIE DES MECANISMES DE PROTECTION
UN EXEMPLE (2)



CONTRÔLES À RÉALISER (1)

- Vérifier lors de l’appel au système de fichiers, que l’utilisateur a le droit d’écriture sur le fichier.

Un pirate peut essayer de déposer directement une requête dans le tampon ou exécuter directement une entrée sortie sur le disque.

- Vérifier que seul une procédure système E/S peut écrire sur le tampon et que seul le gestionnaire de périphérique peut faire des E/S physiques

CONTRÔLES À RÉALISER (2)

Un pirate peut tenter de modifier la structure de donnée qui définissent les différents droits. Soit en appelant la procédure qui est normalement utilisée pour modifier les droits, soit en essayant d'accéder directement à cette structure en mémoire.

- Contrôler le droit d'exécuter les procédures système et contrôler que seules les procédures systèmes ayant des droits adéquats peuvent accéder en lecture ou en modification aux descripteurs des droits.

Le pirate peut essayer de modifier le code exécutable qui assure l'un des contrôles pour le rendre plus permissif.

- Contrôler que tous les éléments de code critique ne peuvent être modifiés en mémoire.

NECESSITE DE LA HIERARCHIE DES MECANISMES

Si (Condition) Alors autoriser action

Un virus pourrait modifier un tel programme de contrôle d'accès:

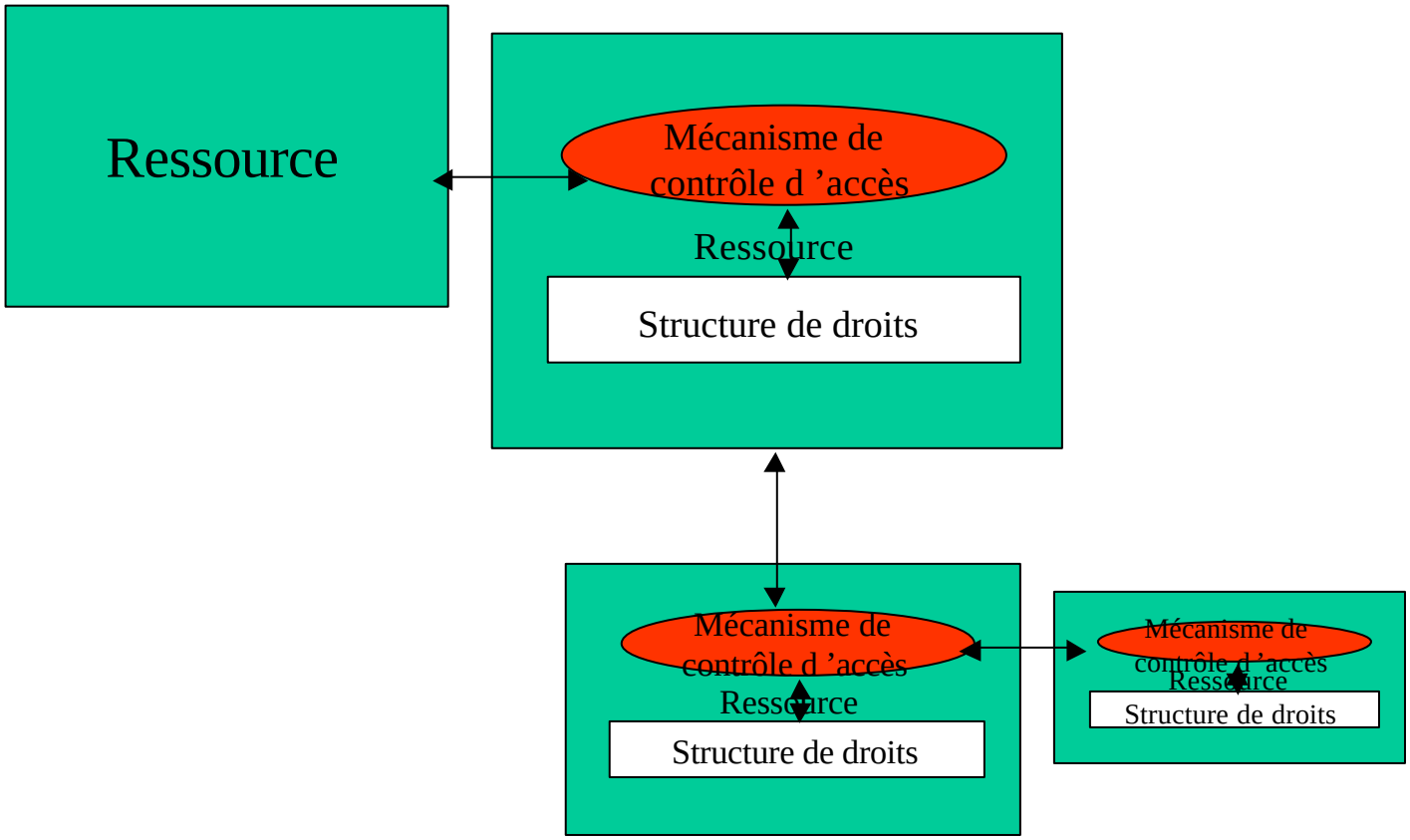
Si c'est moi Alors autoriser l'action

Le maillon faible est l'élément le plus bas : celui qui peut modifier les mécanismes qui servent à contrôler tous les contrôles peut tout modifier.

Ces mécanismes ne doivent pas pouvoir être modifiés par une opération logicielle : *seule une intervention physique sur le matériel doit permettre d'altérer ces mécanismes.*

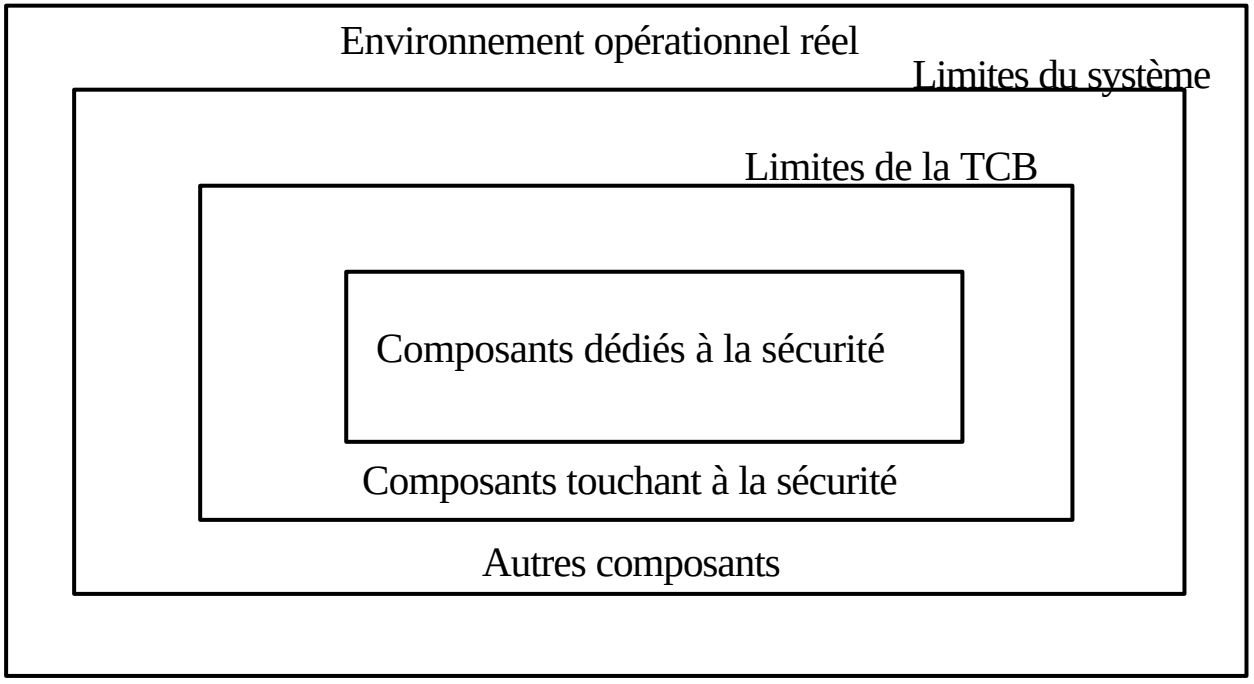
On est ramené à des problèmes de sécurité physique et organisationnelle : qui a accès aux ordinateurs.

HIERARCHIE DES MECANISMES



NOYAU DE SECURITE
ET
MONITEUR DE REFERENCE (1)

L'implantation des mécanismes de sécurité est basé sur une hiérarchie des fonctions (ITSEC)



NOYAU DE SECURITE
ET
MONITEUR DE REFERENCE (2)

Les composants dédiés à la sécurité reposent sur un moniteur de sécurité qui va assurer le contrôle d'accès. Celui ci constitue les niveaux de contrôle de la hiérarchie de protection

Le moniteur doit être

- **inviolable,**
- **incontournable,**
- **correct (par rapport à un ensemble de propriété permettant d'implanter des politiques de sécurité)**

Le moniteur de référence est le "méta guichet" qui permet de gérer des guichets et les droits d'accès aux guichets

NOYAU DE SECURITE
ET
MONITEUR DE REFERENCE (3)

Un moniteur de référence est construit selon une hiérarchie de mécanismes dont l'étanchéité dépend du type d'attaque:

Sur chaque machine il s'agit de mécanismes matériels liés à l'adressage et à l'exécution de certaines instructions. Pour contourner ces mécanismes il faut modifier le matériel:

- Gestion de la mémoire
- Mode d'exécution des processus et contrôle d'accès aux instructions privilégiées
- Code en mémoire morte
- Système matériel d'authentification (lecteur de carte à puces par exemple)

En outre ans un système réparti, une partie du moniteur est composé de protocoles de sécurité

MECANISMES MATERIELS POUR LE NIVEAU BAS

• Les instructions de base de la machine et des périphériques ne doivent pas pouvoir être modifiées. Plus cette notion sera étendue plus facile sera la protection. (utiliser des périphériques spéciaux pour réaliser les opérateurs cryptographiques.)

• Le code d'initialisation du système et les structures définissant les droits de base non modifiables implantés en mémoire morte.

• La mémoire centrale doit être segmentée. Lors de l'exécution de chaque instruction le processeur doit vérifier, selon la nature de l'instruction, si le processus appelant a le droit d' exécuter, lire ou écrire sur chaque segment de mémoire référencé.

•Le droit d'exécuter certaines instructions de base de la machine (comme les accès physique au périphériques) peut être également contrôlé lors de chaque appel (peut être remplacé par une utilisation fine de la mémoire et du chargement: n'accorder le droit d'exécution sur un segment de mémoire contenant des instructions privilégiées qu'à des processus privilégiés).

MACHINES A ANNEAUX DE PROTECTION (1)

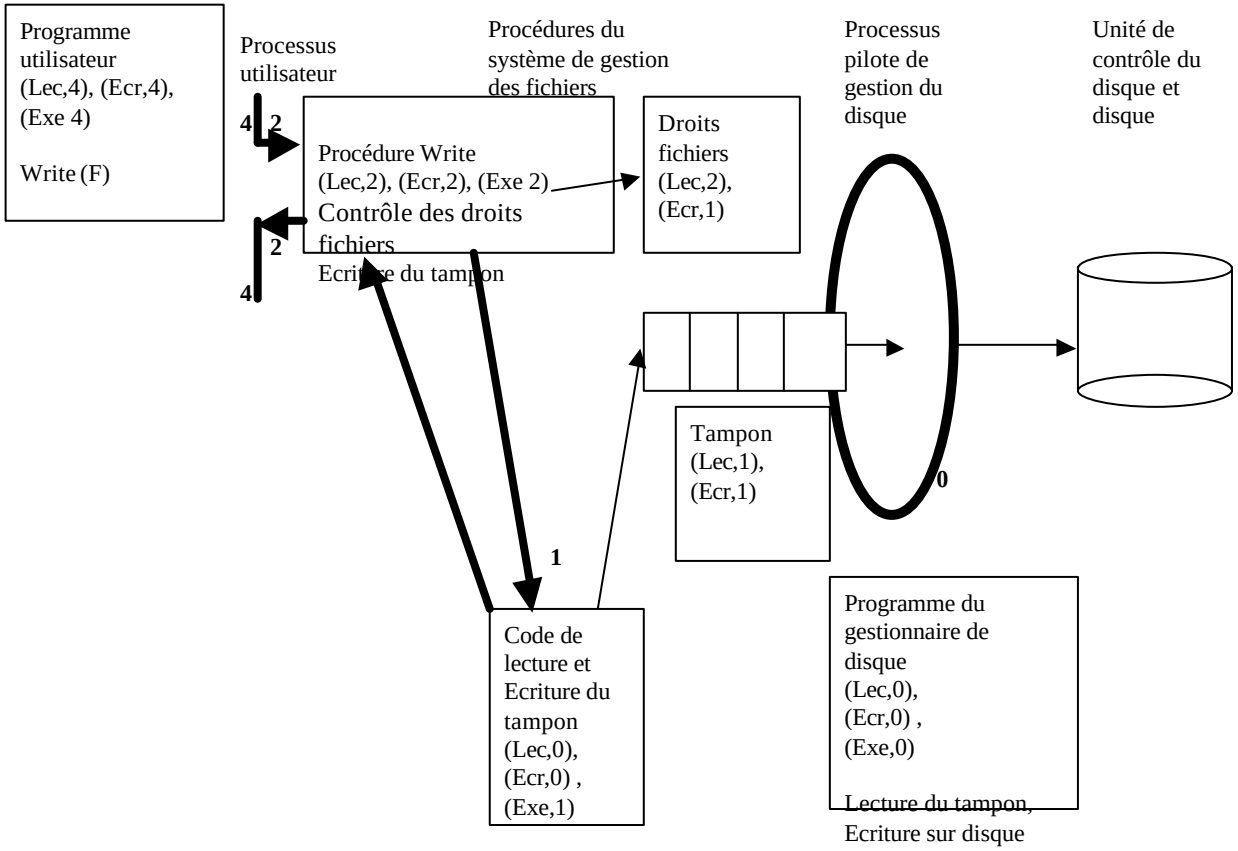
A chaque instant un processus s'exécute dans un contexte donné, les contexte étant hiérachisés (Anneaux de protection)
Un niveau est associé à chaque instruction machine et à chaque référence mémoire (segment ou page)

Certaines instructions ne sont exécutables que dans le domaine le plus privilégié, en particulier celles qui définissent le droit d'accès à une référence mémoire en lecture, écriture ou exécution.

MACHINES A ANNEAUX DE PROTECTION (2)

- L'appel d'une opération (type d'instruction, référence mémoire) implique le contrôle du droit d'accès à l'instruction ou à la référence (le niveau d'appel doit être supérieur ou égal à celui de l'objet référencé). Sinon il y a déroutement.
- Le déroutement provoque un accès à un guichet : Il doit s'agir d'un appel à une instruction privilégiée de changement d'anneau, qui va provoquer l'exécution d'un code de contrôle du droit dans le domaine appelé et une acceptation ou un rejet.

MACHINES A ANNEAUX DE PROTECTION (3)



MACHINES A DOMAINES

A un objet est associé un espace qui lui soit propre : son **domaine** de protection.

- Tant que l'exécution du code de cet objet référence des adresses qui sont situées dans son espace propre, il ne se passe rien de particulier.
- Dès que l'objet référence une adresse à l'extérieur de son espace, il y a déroutement de l'exécution et vérification du fait que la référence externe est une demande d'exécution d'une méthode d'un autre objet. Si ce n'est pas l'instruction n'est pas réalisée.
- Dans le cas contraire, il y a copie des paramètres d'appel du domaine de l'appelant vers le domaine de l'appelé. Et d 'une capacité à exécuter la méthode.
- La première opération que réalise la méthode appelée est de vérifier la validité de la capacité. Si celle si est valide la méthode est exécutée.

PROPRIETES DES CAPACITES

- Elle doit être intègre : seul l’objet qui peut donner un droit doit être capable de la fabriquer ou de la modifier,
- Elle doit avoir une portée limitée soit en terme du nombre d’exécutions de la méthode qu’elle autorise soit en terme de durée.
- Elle doit permettre de déterminer si le détenteur de la capacité a le droit de propager le droit contenu dans la capacité et dans quelle limite.
- En principe elle ne doit pas pouvoir être copiée.

IMPLANTATION DES CAPACITES

- Dans les machines à capacités propriétés sont assurées par un mécanisme partiellement matériel et partiellement logiciel qui gère les capacités dans un domaine propre.
- Dans un système réparti une capacité est un élément du message transmis par l'appelant signé par l'objet qui est habilité à délivrer les droits.

  Peut comporter des indications de limite de validité et de droit de propagation.

  L'appelant peut également signer le message complet permettant son authentification par l'appelé.

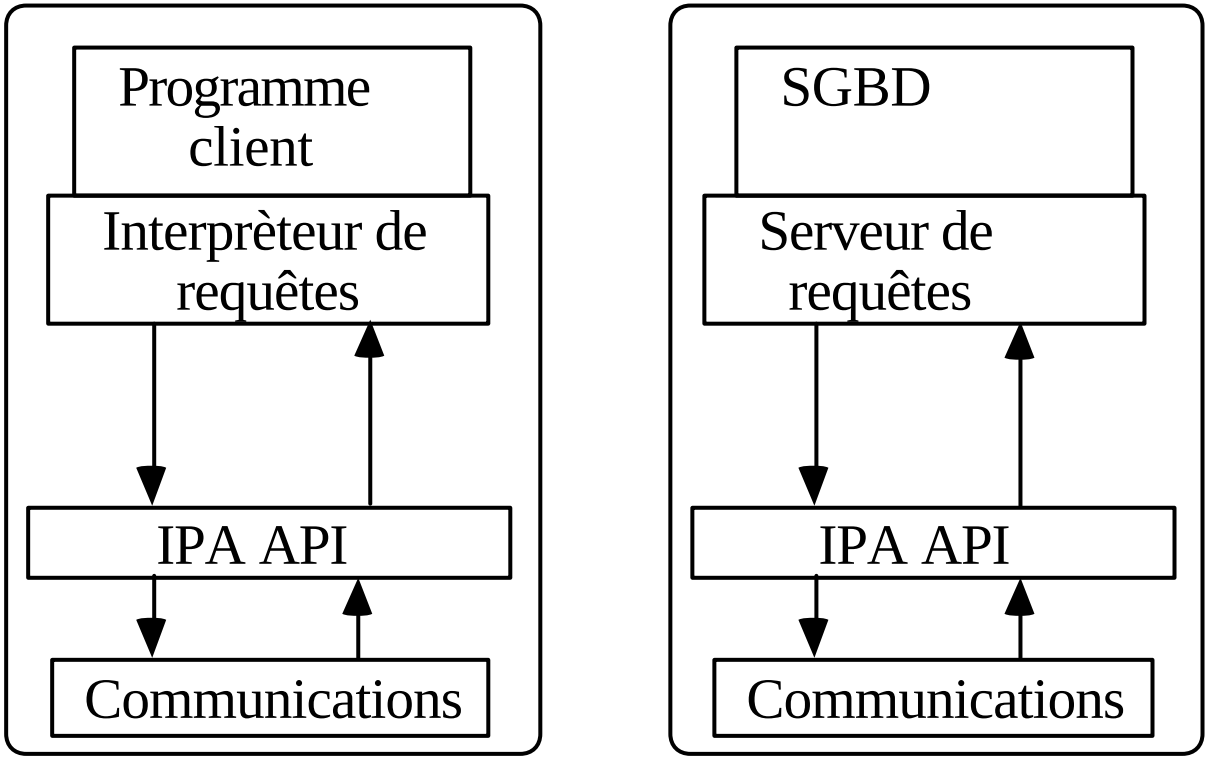
  Cette solution a pratiquement toutes les propriétés requises, mais ne permet pas d'éviter la copie.

L ’APPEL DE PROCEDURE A DISTANCE SECURISE

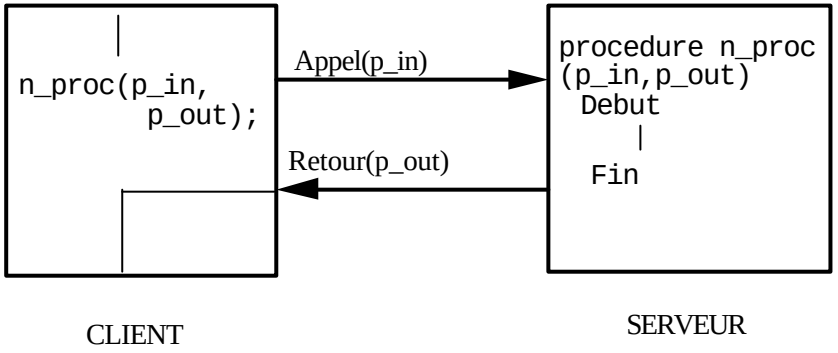
Le service d ’appel de procédure à distance (APD/RPC)

- Présentation **syntaxique et sémantique** du mécanisme précédent **en terme d'appel de procédure distante.**
- A travers un API simulant l ’appel de procédure local:
  - synchrone
  - sans mémoire

Les API client/serveur



Fonctionnement de l ’APD



La souche client

C’est la procédure d’interface du site client:

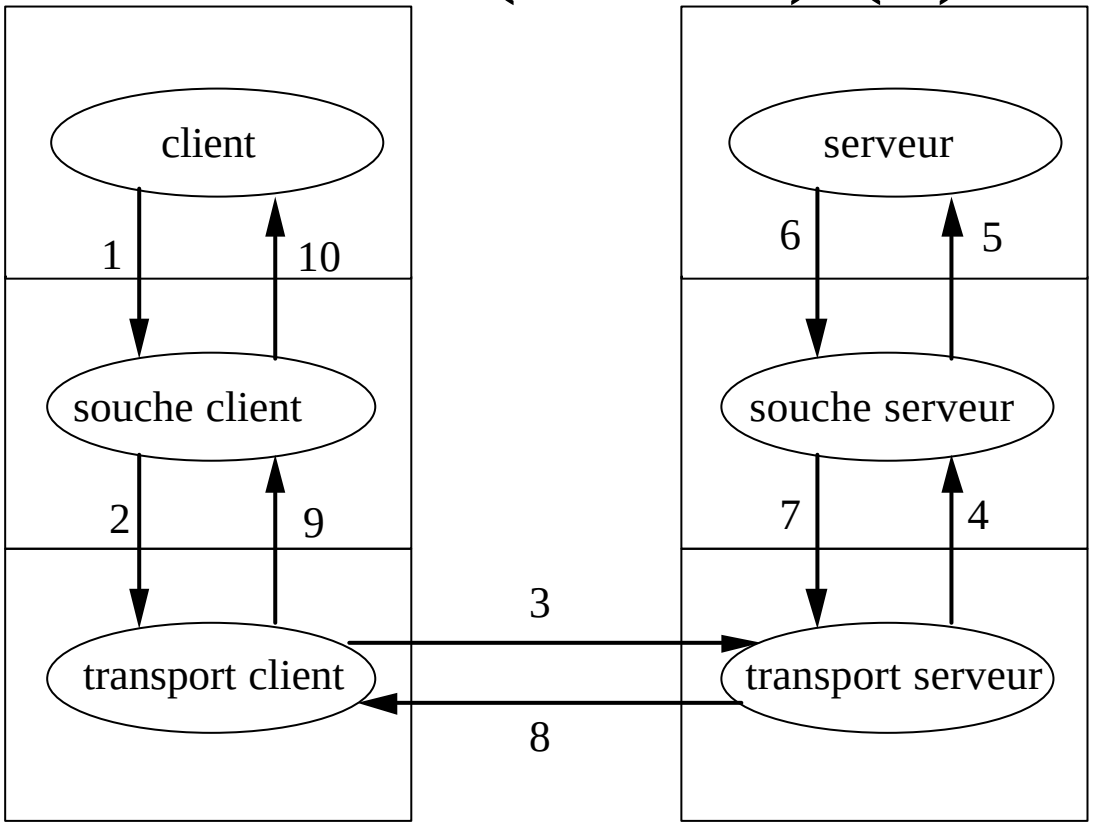
- qui reçoit l’appel en mode local
- le transforme en appel distant
- en envoyant un message.
- reçoit les résultats après l'exécution
- retourne les paramètres résultats comme dans un retour de procédure.

La souche serveur

C’est la procédure sur le site serveur qui:

- reçoit l’appel sous forme de message,
- fait réaliser l’exécution sur le site serveur par la procédure serveur
- retransmet les résultats par message.

Implantation de l ’APD par souches (STUB) (1)



Détails des étapes (1)

Étape 1

- Le client réalise un appel procédural vers la procédure souche client.

- La souche client collecte les paramètres , les assemble dans un message **(“parameter marshalling”).**

Étape 2

- La souche client détermine l’adresse du serveur.

- La souche client demande à une entité de transport locale la transmission du message d'appel.

Étape 3

- Le message est transmis sur un réseau au site serveur.

Détails des étapes (2)

Étape 4

- Le message est délivré à la souche du serveur.

Étape 5

- La souche serveur désassemble les paramètres, et réalise l’appel effectif de la procédure serveur.

Étape 6

- La procédure serveur ayant terminé son exécution transmet à la souche serveur dans son retour de procédure les paramètres résultats.La souche serveur collecte les paramètres retour, les assemble dans un message (“parameter marshalling”).

Détails des étapes (3)

Étape 7

- La procédure souche serveur demande à l'entité de transport locale la transmission du message.

Étape 8

- Le message est transmis sur un réseau au site client.

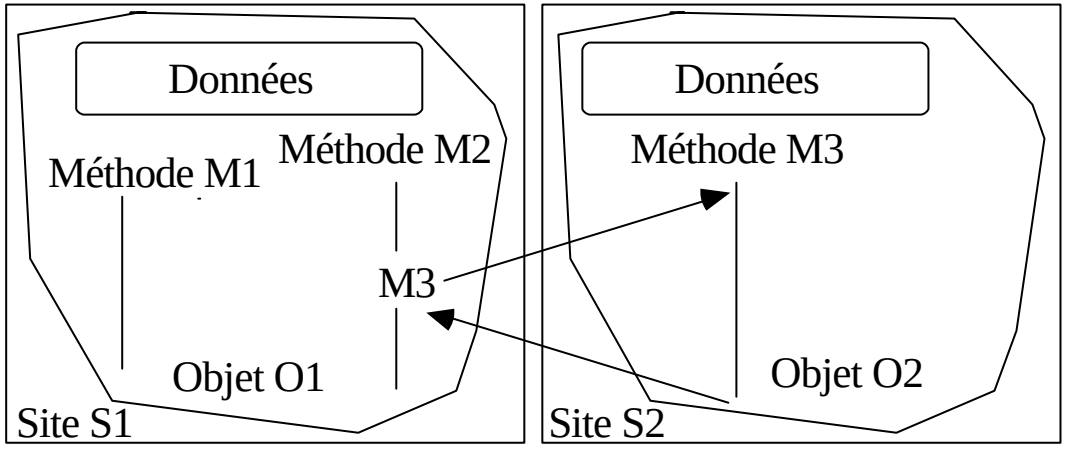
Étape 9

- Le message est délivré à la souche du client. La souche client désassemble les paramètres retour.

Étape 10

- La procédure souche client transmet les résultats au client en effectuant le retour final de procédure.

Objets répartis



Objectifs de l ’APD sécurisée

- Répartir la notion de machine à domaines
- En utilisant des messages de capacités ou de ticket
- Eventuellement dans un contexte d ’objets répartis
- Les étapes de l ’APD incluent des fonctions de sécurité

Etapes 1 de l ’APD Sécurisé

Etape 1: L ’appel provoque un déroutement local car c ’est une référence hors du domaine de l ’appelant.

L ’appelant passe une capacité (ou un ticket) avec les paramètres d ’appel

Etape 2, 3 et 4 de l ’APD Sécurisé

La souche client ouvre une connexion sécurisée avec la souche serveur, avec authentification des deux entités, protection en intégrité et éventuellement en confidentialité (SSL par exemple)

Les paramètres et la capacités sont transmis sur cette connexion

Etapes 5 et 6
de l ’APD Sécurisé

La souche serveur appelle l’objet local en passant la capacité ou le ticket

L ’objet local contrôle les droits et exécute la méthode

Etapes 8, 9 et 10
de l ’APD Sécurisé

La souche serveur ouvre une connexion sécurisée avec la souche client, et retourne les paramètres