Calculabilité. Devoir à rendre au plus tard le 16 octobre 2017

Contrôles d'accès et politiques de sécurité

L'objet du problème est d'étudier des systèmes de contrôle d'accès, typiquement ceux qui sont utilisés dans les systèmes d'exploitation. Dans la suite U désignera un ensemble (infini) d'*utilisateurs*, $O \supseteq U$ un ensemble d'*objets* et R un ensemble fini de *droits*.

Dans la suite, si σ est une application d'une séquence de variables $\vec{x}$ dans un ensemble E et e est une expression contenant des variables de $\vec{x}$, $e\sigma$ désigne l'expression e dans laquelle chaque variable $x \in \vec{x}$ est substituée par $\sigma(x)$.

Un système de contrôle d'accès (SCA) est défini par un ensemble fini d'utilisateurs $u \subseteq U$, un ensemble fini d'objets $o \subseteq O$, contenant u, et une matrice D de droits d'accès, qui, à chaque utilisateur et chaque objet associe un sous-ensemble de R.

Un ensemble fini de *commandes* permettent de modifier la matrice des droits d'accès. C'est la *politique de sécurité*. De manière générale, une commande c est paramétrée par un nombre fini de variables $\vec{x} = x_1, \ldots, x_n$ de type O et est définie par:

- $\mathsf{PRECOND}_c(\vec{x}) \subseteq \vec{x} \times \vec{x} \times R$
- $\mathsf{NEWU}_c(\vec{x}) \subseteq \vec{x}$
- $\mathsf{NEWO}_c(\vec{x}) \subseteq \vec{x}$
- $\mathsf{DELO}_c \subseteq \vec{x}$
- $\mathsf{DELU}_c \subseteq \vec{x}$
- $\mathsf{GRANT}_c(\vec{x}) \subseteq \vec{x} \times \vec{x} \times R$
- $\mathsf{REM}_c(\vec{x}) \subseteq \vec{x} \times \vec{x} \times R$

Les commandes agissent sur les SCA de la manière suivante. Si $(u, o, D$ est un SCA, c une commande paramétrée par $\vec{x}$ et σ est une application de $\vec{x}$ dans O, l'effet de la commande $c\sigma$ sur (u, o, D) est un SCA (u', o', D') défini comme suit:

1. Si $\exists (a, b, r) \in \mathsf{PRECOND}_c(\vec{x})\sigma$, $(a, b) \notin u \times o$ ou $r \notin D(a, b)$, alors la commande est sans effet.
2. Si $\mathsf{NEWU}_c(\vec{x})\sigma \cap u \neq \emptyset$ ou $\mathsf{NEWO}_c(\vec{x})\sigma \cap o \neq \emptyset$ ou $\mathsf{DELU}_c(\vec{x})\sigma \not\subseteq u$ ou $\mathsf{DELO}_c(\vec{x})\sigma \not\subseteq o$, la commande est sans effet.

   Sinon, soient $u' = (u \cup \mathsf{NEWU}_c(\vec{x})\sigma) \setminus \mathsf{DELU}_c(\vec{x})\sigma$, $o' = (o \cup \mathsf{NEWO}_c(\vec{x})\sigma \cup \mathsf{NEWU}_c(\vec{x})\sigma) \setminus \mathsf{DELO}_c(\vec{x})\sigma$. Soit D' défini par $D'(a, b) = D(a, b)$ si $(a, b) \in (u \cap u') \times (o \cap o')$ et $D'(a, b) = \emptyset$ si $(a, b) \in (u' \times o') \setminus (u \times o)$.
3. $\forall (a, b, r) \in \mathsf{REM}_c(\vec{x})\sigma$, si $(a, b) \notin u' \times o'$, la commande est sans effet. Sinon, r est retiré de $D'(a, b)$
4. $\forall (a, b, r) \in \mathsf{GRANT}_c(\vec{x})\sigma$, si $(a, b) \notin u' \times o'$, la commande est sans effet. Sinon, r est ajouté à $D'(a, b)$.

Question 0

Soient $u = o = \{\mathsf{root}, \mathsf{alice}, \mathsf{charlie}\}$ et $D(x, x) = R = \{\mathsf{o}, \mathsf{c}, \mathsf{r}, \mathsf{w}, \mathsf{d}\} = D(\mathsf{root}, x)$ pour tout $x \in u$.

La politique de sécurité est donnée par les commandes suivantes:

	PRECOND	NEWU	NEWO	DELU	DELO	GRANT	REM
$\mathsf{newu}_S(x, y, z)$	(x, y, c)	z	z	$-$	$-$	$(y, z, s), s \in S$	$-$
	$(x, y, s), s \in S$	$-$	$-$	$-$	$-$		$-$
$\mathsf{chmod}_{+s}(x, y)$	(x, y, o)	$-$	$-$	$-$	$-$	(x, y, s)	$-$
$\mathsf{chmod}_{-s}(x, y)$	(x, y, o)	$-$	$-$	$-$	$-$	$-$	(x, y, s)
$\mathsf{remu}(x, y)$	(x, y, d)	$-$	$-$	y	y	$-$	$-$

Montrer que les utilisateurs alice et charlie peuvent avoir tous deux les mêmes droits sur certains objets.

Question 1

Montrer que le problème suivant est indécidable:

Donnée: un SCA (u, o, D), un ensemble fini de droits R, une politique de sécurité, un utilisateur $a \in u$, un objet $b \in o$, une permission $r \in R$.

Question: Existe-t-il une suite d'instances de commandes qui conduit à un SCA dans lequel a possède la permission r pour l'objet b ?

Question 2

Dans cette question, l'ensemble de droits R est fixé.

Montrer qu'il existe un ensemble de droits R pour lequel le problème suivant est indécidable:

Donnée: un SCA (u, o, D), une politique de sécurité, un utilisateur $a \in u$, un objet $b \in o$, une permission $r \in R$.

Question: Existe-t-il une suite d'instances de commandes qui conduit à un SCA dans lequel a possède la permission r pour l'objet b ?

Question 3

Dans cette question, l'ensemble de droits R et la politique de sécurité sont fixés.

Montrer qu'il existe un ensemble de droits R et une politique de sécurité pour lesquels le problème suivant est indécidable:

Donnée: un SCA (u, o, D), un utilisateur $a \in u$, un objet $b \in o$, une permission $r \in R$.

Question: Existe-t-il une suite d'instances de commandes qui conduit à un SCA dans lequel a possède la permission r pour l'objet b ?

Question 4

On s'interdit ici les commandes pour lesquelles $\mathsf{NEWU} \neq \emptyset$ (autrement dit, on ne peut pas créer d'utilisateur). En revanche, on ajoute dans la définition d'une commande c un ensemble $\mathsf{UNSET}_c \subseteq \vec{x}$, avec la sémantique suivante:

> Si $\exists(a, b, r) \in \mathsf{UNSET}_c(\vec{x})\sigma$ et $r \in D(a, b)$, alors la commande est sans effet

Autrement dit les préconditions ne sont plus seulement l'existence de droits mais aussi l'absence de droits.

Montrer qu'il existe un ensemble de droits tel que le problème suivant est indécidable:

Donnée: une politique de sécurité qui ne permet aucune création d'utilisateur, $a \in U, b \in O, r \in R$

Question: pour tout SCA (u, o, D) tel que $a \in u, b \in o$, il existe une suite de commandes qui conduit à octroyer la permission r à a pour l'objet b.