

Un cadre sémantique pour le contrôle d'accès

Mathieu Jaume* — Charles Morisset**

* SPI LIP6 UPMC
104 av. du Président Kennedy, 75016, Paris, France
Mathieu.Jaume@lip6.fr

** UNU-IIST, P.O. Box 3058, Macao SAR, China
Charles.Morisset@iist.unu.edu

RÉSUMÉ. Un des aspects de la sécurité des systèmes d'information concerne le contrôle des accès aux données d'un système pour lequel différentes politiques de sécurité peuvent être mises en œuvre. Toutefois, rien ne sert de mettre en place une politique de sécurité pour gérer un système si les programmes chargés de garantir le bon fonctionnement de cette politique ne sont pas fiables. Ne pas apporter de garanties fortes sur la correction de tels programmes reviendrait à construire un château fort avec une porte en papier. Nous utilisons les méthodes formelles pour aborder le contrôle d'accès en introduisant un cadre sémantique abstrait permettant de spécifier, d'implanter et de comparer des politiques. Ce cadre permet d'identifier les « ingrédients » d'une politique de contrôle d'accès et caractérise des propriétés de simulation entre implantations permettant d'exprimer une notion de restriction entre politiques.

ABSTRACT. One of the aspects of computer security relates to the control of the access to the data of a system for which various security policies can be enforced. However, it is useless to set up a security policy if the programs enforcing such a policy are not sound. Not to bring strong guarantees on the correction of such programs would amount building a stronghold with a paper door. We use the formal methods to deal with access control by introducing an abstract semantical framework designed for the specification, the implementation and the comparison of policies. This framework identifies the “ingredients” of an access control policy and characterizes a simulation relationship between implementations making it possible to express that a policy is more restrictive than another one.

MOTS-CLÉS : Contrôle d'accès, Méthodes formelles, Sémantique, Sécurité

KEYWORDS: Access control, Formal Methods, Semantics, Security

1. Introduction et motivations

Selon Vinton Cerf, cofondateur du protocole TCP/IP, entre 100 et 150 millions des 600 millions d'ordinateurs connectés à internet sont actuellement sous le contrôle direct de pirates¹. Ces ordinateurs sont utilisés à l'insu de leur propriétaire légitime afin d'effectuer toutes sortes d'actions illégales, comme l'envoi de « spam » ou des attaques contre des serveurs. Ces réseaux d'ordinateurs « zombies » sont pour le moment essentiellement utilisés à des fins commerciales. Qu'en sera-t-il si ces réseaux sont un jour contrôlés par des organisations mafieuses ou terroristes ? Même s'ils ne sont qu'une estimation, ces chiffres démontrent que si la sécurité devrait être l'affaire de tous, elle est actuellement l'affaire de peu de gens. Force est de constater que la vulnérabilité de nos infrastructures informatiques est actuellement largement sous-estimée, du moins dans les informations mises à la disposition du grand public. Des techniques de spécification, de conception et d'implantation des logiciels, permettant de déjouer les menaces causées par l'usure, existent dans les domaines liés à la sûreté (nucléaire, ferroviaire, aérospatiale, etc.). Il est urgent de mettre en place de tels procédés dans les domaines liés à la sécurité, pour déjouer les menaces relatives aux attaques informatiques.

Paradoxalement, bien que la vulnérabilité des infrastructures soit sous-estimée, les utilisateurs font preuve de méfiance vis-à-vis des nouvelles technologies. En effet, comment s'assurer qu'un programme va effectuer les opérations demandées ? Comment être sûr qu'il ne va pas permettre à n'importe qui d'accéder à des informations sensibles ? Cette confiance est primordiale, car sans elle, le système n'est pas utilisé par les clients. Ces questions sont d'autant plus pertinentes que l'intégration des communications réseaux dans les grands systèmes informatiques abolit toute notion de barrière physique de protection. Il est difficile, pour un produit, d'obtenir la confiance du grand public. Cette confiance passe généralement par un certain nombre d'avis de personnes reconnues comme experts. Ces experts se basent sur des protocoles ou des normes pour certifier que le produit en question est conforme aux exigences issues de la demande de confiance. Dans le domaine du logiciel, les Critères Communs (CC, 2006) (recueil de normes définies par des agences gouvernementales) fournissent une méthodologie permettant d'atteindre des hauts niveaux de sécurité. Ils définissent à la fois un cadre de travail pour la conception et la réalisation de logiciels et une référence pour les utilisateurs de ces logiciels. Les hauts niveaux de sûreté des critères communs (EAL – *Evaluation Assurance Level* – 5 à 7) requièrent l'utilisation de méthodes formelles dans les étapes de spécification et de conception du logiciel. Cette préconisation des méthodes formelles vient du besoin de recourir, comme dans toutes les autres disciplines scientifiques, à des modèles et formalismes mathématiques pour mieux comprendre et analyser le problème. P. Amey définit la « chose formelle » comme une « chose soutenue par une rigueur mathématique » (Amey, 2004). Ainsi, les méthodes formelles peuvent être vues comme des « méthodes soutenues par une rigueur mathématique », dépourvues d'ambiguïté, pour spécifier et dans certains cas

1. Article de la BBC du 25/01/07.

implanter un système en garantissant que certaines propriétés sont respectées. Lorsqu'il s'agit de systèmes logiciels critiques, ces propriétés peuvent être vitales.

Dans cet article, nous utilisons une démarche formelle pour étudier certaines des propriétés classiques de sécurité des systèmes d'information. Selon les critères communs, un système est vu comme une installation donnée de technologies de l'information, avec un objectif et un environnement opérationnel particuliers et une politique de sécurité est un ensemble de règles qui précisent comment gérer, protéger ou distribuer les informations ou ressources du système. Nous nous intéressons ici plus particulièrement aux politiques de contrôle d'accès dont l'objectif est de régir et gérer les accès effectués selon certains modes (lecture, écriture, etc.) par des sujets, les entités actives (processus, programmes, utilisateurs, etc.) sur des objets, les entités passives (données, fichiers, programmes, etc.). Mettre en place un mécanisme de contrôle d'accès consiste dans un premier temps à définir la politique de contrôle d'accès à proprement parler, c'est-à-dire spécifier les accès autorisés et ceux interdits. Dans un deuxième temps, il faut définir un moniteur de référence, c'est-à-dire le programme chargé de mettre en œuvre la politique de contrôle d'accès au sein du système. Toujours selon les critères communs, un moniteur de référence doit posséder les trois caractéristiques suivantes :

- des sujets non sûrs ne peuvent pas interférer avec son fonctionnement, *i.e.* il est à l'épreuve d'une intrusion physique ;
- des sujets non sûrs ne peuvent pas court-circuiter les contrôles qu'il effectue, *i.e.* il est systématiquement appelé ;
- il est suffisamment simple pour être analysé et pour comprendre son comportement, *i.e.* sa conception est simple.

Ces trois caractéristiques, introduites dans (Anderson, 1972), sont connues sous l'acronyme *NEAT*, pour *Non-bypassable* (il n'est pas possible d'éviter les fonctions de sécurité), *Evaluatable* (les fonctions de sécurité sont suffisamment simples pour être mathématiquement vérifiées et évaluées), *Always Invoked* (les fonctions de sécurité sont tout le temps appelées) et *Tamperproof* (les fonctions de sécurité ne peuvent pas être altérées). Cet acronyme est défini dans le cadre de *MILS*² (*Multiple Independent Levels of Security*), une approche de développement de systèmes sécurisés. L'utilisation de méthodes formelles pour la conception d'un moniteur de référence facilite son évaluation et sa vérification, puisque la correction du programme vis-à-vis de sa spécification peut être énoncée et prouvée de manière formelle.

De nombreux modèles de contrôle d'accès existent dans la littérature, comme le modèle BLP (Bell *et al.*, 1973), le modèle HRU (Harrison *et al.*, 1976), le modèle de la Muraille de Chine (Brewer *et al.*, 1989), celui à base de rôles (Ferraiolo *et al.*, 1992), sans oublier un ensemble « d'extensions » de ce dernier, comme le modèle à base d'organisations (Kalam *et al.*, 2003), à base de coalition (Cohen *et al.*, 2002), à base d'équipes (Thomas, 1997), etc. Chacun de ces modèles a été conçu pour répondre à

2. <http://www.ois.com/MILS/>

un besoin de sécurité précis dans un contexte précis. Néanmoins, certains de ces modèles ne sont pas exprimés de manière formelle, ce qui peut conduire à une mauvaise compréhension, une mauvaise utilisation, voire à une mauvaise implantation de ces modèles. De plus, ces différents modèles ne sont pas tous exprimés dans un même formalisme, et il est ainsi difficile de comparer deux modèles entre eux. Nous présentons donc ici un cadre formel uniforme permettant la spécification, l'implantation et la comparaison de modèles de contrôle d'accès.

La suite de cet article est organisée comme suit. La section 2 présente le cadre sémantique permettant de spécifier et d'implanter les modèles de contrôle d'accès. Ensuite, nous introduisons des critères à partir desquels nous pouvons définir des relations de comparaison entre implantations d'un modèle mais aussi entre modèles (section 3). Enfin, dans la section 4, nous terminons cet article en illustrant l'utilisation des concepts précédemment introduits avec des exemples classiques de modèles de contrôle d'accès. Cet article synthétise les travaux décrits dans (Morisset, 2004; Jaume *et al.*, 2005; Blond *et al.*, 2006; Blond *et al.*, 2007; Jaume *et al.*, 2006a; Jaume *et al.*, 2006b; Jaume *et al.*, 2007; Morisset, 2007). Nous ne donnons ici aucune preuve, elles peuvent toutes être trouvées dans (Morisset, 2007).

2. Cadre sémantique

Nous introduisons ici un cadre permettant non seulement de spécifier et d'implanter des modèles de contrôle d'accès mais aussi de les comparer. Il s'agit d'identifier les « ingrédients » communs aux modèles de contrôle d'accès, d'exprimer les propriétés génériques qu'ils vérifient et de comprendre le rôle de ces « ingrédients » dans une implantation. Le cadre que nous introduisons ne définit toutefois pas un langage de spécification de modèles de contrôle d'accès mais fournit plutôt une spécification abstraite de ce qui constitue un modèle. Il s'agit donc d'un *cadre sémantique pour le contrôle d'accès*.

2.1. Politiques de contrôle d'accès

Une politique de sécurité permet de caractériser les états d'un système et de spécifier ce qu'est un état sûr du système. Nous introduisons tout d'abord les différents concepts entrant en jeu dans la définition d'une politique, puis nous donnons quelques propriétés générales sur les politiques de sécurité. Nous illustrons ici les différentes définitions par un exemple d'un système de gestion des ressources (imprimantes, scanners, etc.) au sein d'un réseau.

2.1.1. Définition

Entités. Les entités du système peuvent être réparties dans deux ensembles : l'ensemble \mathcal{S} des sujets, également appelés *entités actives*, qui correspondent aux entités qui effectuent les actions dans le système, et l'ensemble \mathcal{O} des objets, également appe-

lés *entités passives*, qui subissent les actions. Les sujets et les objets sont généralement considérés comme des entités atomiques. Ces deux ensembles ne sont pas nécessairement disjoints : par exemple, un processus peut à la fois être un sujet et ainsi effectuer des opérations, et un objet, dans le cas où un autre processus tente de l'arrêter.

Accès. Nous introduisons ici l'ensemble \mathcal{A} des modes d'accès qui caractérisent les différents types d'accès effectués par les sujets sur les objets. Cet ensemble contient généralement *read*, *write*, *append*, etc. Une approche classique consiste à représenter un accès par un triplet (s, o, x) , signifiant que le sujet s accède à l'objet o selon le mode d'accès x . Néanmoins, d'autres approches existent (on peut par exemple regrouper les modes d'accès, ou encore considérer les accès conjoints de sujets sur des objets). Afin de pouvoir prendre en compte ces différentes situations, nous nous limitons à noter \mathbb{A} l'ensemble de tous les accès, sans tenir compte de leur représentation.

EXEMPLE. Considérons un système de gestion des ressources. L'ensemble $\mathcal{S}_e = \{s_1, s_2, \dots, s_n\}$ représente les utilisateurs du réseau, et l'ensemble $\mathcal{O}_e = \{o_1, o_2, \dots, o_m\}$ représente les ressources (imprimantes, stockage réseau, scanners, etc.). L'ensemble \mathbb{A}_e est défini comme le produit cartésien $\mathcal{S}_e \times \mathcal{O}_e \times \mathcal{A}_e$, où $\mathcal{A}_e = \{\text{read}, \text{write}\}$.

Paramètres de sécurité. Il est souvent nécessaire d'associer de l'information aux entités afin de pouvoir exprimer la politique de sécurité, et également de décrire précisément le système. Ces informations sont construites à partir de ce que nous appellerons les paramètres de sécurité. Par exemple, dans le modèle de Bell et LaPadula, le paramètre de sécurité est un treillis de niveaux de sécurité, tandis que dans le modèle de la Muraille de Chine, ces paramètres correspondent aux classes de conflit d'intérêt. Les paramètres de sécurité sont désignés par ρ .

EXEMPLE (SUITE). Chaque utilisateur et chaque ressource peut appartenir à une ou plusieurs équipes de travail (comptabilité, ressources humaines, etc.), et nous introduisons le paramètre de sécurité $\rho_e = \{t_1, t_2, \dots, t_k\}$, où chaque t_i représente un nom d'équipe.

Etats. Les systèmes de contrôle d'accès sont ici modélisés sous la forme de machines à états. Un état représente le système à un instant donné et contient au moins une description de l'ensemble des *accès courants*, c'est-à-dire de tous les accès qui ont été acceptés et qui n'ont pas encore été relâchés. L'ensemble des états est noté Σ . De plus, un état doit également définir un ensemble de *fonctions de sécurité*, qui relient les différentes entités aux paramètres de sécurité. Dans le modèle de Bell et LaPadula, ces fonctions de sécurité correspondent aux fonctions qui associent un niveau de sécurité aux sujets et aux objets. Etant donné que ces fonctions de sécurité sont spécifiées par les états, elles peuvent être modifiées lors de transitions, contrairement aux paramètres de sécurité, qui sont fixes pour une politique donnée. Par exemple, il est possible de changer le niveau de sécurité d'un sujet dans le modèle de Bell et LaPadula (ce changement n'est toutefois pas explicite dans le modèle original), mais il n'est pas possible de rajouter ou d'enlever un niveau de sécurité dans le treillis. Si nous voulions concevoir un modèle permettant de modifier dynamiquement le treillis

des niveaux de sécurité, il suffirait de considérer ce treillis non plus comme un paramètre de sécurité mais comme une fonction de sécurité. Aussi, on peut définir deux fonctions sur les états :

$$\Lambda : \Sigma \rightarrow \wp(\mathbb{A}) \quad \Upsilon : \Sigma \rightarrow \mathbf{SF}$$

où $\wp(\mathbb{A})$ désigne l'ensemble des parties de \mathbb{A} . Etant donné un état σ , $\Lambda(\sigma)$ représente l'ensemble des accès courants du système dans l'état σ et $\Upsilon(\sigma)$ représente l'ensemble des fonctions de sécurité de l'état σ . Notons que la « structure » de l'ensemble \mathbf{SF} des fonctions de sécurité n'est pas spécifiée à ce niveau.

EXEMPLE (SUITE). La fonction $t_s : \mathcal{S}_e \rightarrow \wp(\rho_e)$ (resp. $t_o : \mathcal{O}_e \rightarrow \wp(\rho_e)$) associe à chaque utilisateur (resp. ressource) un ensemble d'équipes. Un état $\sigma \in \Sigma_e$ est un triplet (m, t_s, t_o) , où $m \in \wp(\mathbb{A}_e)$ est un ensemble d'accès et t_s et t_o sont les fonctions de sécurité introduites ci-avant. Pour un état $\sigma = (m, t_s, t_o)$, on a donc $\Lambda(\sigma) = m$ et $\Upsilon(\sigma) = (t_s, t_o)$.

Prédicat de sécurité. Une politique de sécurité spécifie les états sûrs d'un système. Ces états sûrs sont caractérisés par un prédicat Ω . Nous utilisons dans la suite la logique du premier ordre pour définir ce prédicat, mais d'autres logiques peuvent être utilisées. On note $\Sigma_{|\Omega}$ l'ensemble $\{\sigma \in \Sigma \mid \Omega(\sigma)\}$ des états sûrs.

EXEMPLE (SUITE). La politique considérée pour la gestion de ressources consiste à imposer que si un utilisateur accède à une ressource, alors il doit appartenir à une équipe à laquelle appartient la ressource³ et impose qu'un utilisateur ne puisse accéder à plus de trois ressources différentes en même temps. On définit le prédicat Ω_e ainsi :

$$\Omega_e(\sigma) \Leftrightarrow \left(\begin{array}{l} \forall \sigma = (m, t_s, t_o) \in \Sigma_e \\ \forall s \in \mathcal{S}_e \forall o \in \mathcal{O}_e \forall x \in \mathcal{A}_e \\ (s, o, x) \in m \Rightarrow t_s(s) \cap t_o(o) \neq \emptyset \\ \wedge \forall s \in \mathcal{S}_e \forall x \in \mathcal{A}_e \\ \text{card}(\{o \in \mathcal{O}_e \mid (s, o, x) \in m\}) \leq 3 \end{array} \right)$$

Toutes ces notions nous permettent de définir une politique de contrôle d'accès comme suit.

Définition 1 Une politique de contrôle d'accès $\mathbb{P}[\rho]$, basée sur un paramètre de sécurité ρ , est définie par un quintuplet $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$ où \mathcal{S} est un ensemble non vide de sujets, \mathcal{O} est un ensemble d'objets, \mathcal{A} est un ensemble de modes d'accès, Σ est l'ensemble des états du système sur lequel la politique est mise en œuvre et Ω est le prédicat de sécurité définissant les états sûrs.

EXEMPLE (SUITE). On note $\mathbb{P}_e[\rho_e] = (\mathcal{S}_e, \mathcal{O}_e, \mathcal{A}_e, \Sigma_e, \Omega_e)$ la politique correspondant au système de gestion de ressources.

3. La notion d'équipe est similaire à la notion de « ticket » introduite dans (Levy, 1984).

2.1.2. Propriétés

Afin de pouvoir définir des propriétés sur les politiques de contrôle d'accès, nous introduisons une fonction $\mathcal{W} : \Sigma \rightarrow \wp(\wp(\mathbb{A}))$ qui, étant donné un état σ , retourne les ensembles d'accès qui peuvent être ajoutés à l'ensemble des accès courants de l'état σ , sans changer les fonctions de sécurité, de manière à ce que l'état ainsi obtenu soit sûr.

Définition 2 (Accès potentiels d'un état)

$$\mathcal{W}(\sigma) = \left\{ A \in \wp(\mathbb{A}) \mid \forall \sigma' \in \Sigma \right. \\ \left. (\Upsilon(\sigma') = \Upsilon(\sigma) \wedge \Lambda(\sigma') = \Lambda(\sigma) \cup A) \Rightarrow \Omega(\sigma') \right\}$$

EXEMPLE (SUITE). Considérons des ensembles restreints de sujets $\mathcal{S}'_e = \{s_1, s_2\}$, d'objets $\mathcal{O}'_e = \{o_1, o_2, o_3, o_4\}$ et de noms d'équipes $\rho'_e = \{t_1, t_2\}$. Nous ne considérons dans cet exemple que les accès en lecture (c'est-à-dire $\mathcal{A}'_e = \{\text{read}\}$). Soit $\sigma_1 = (m_1, t_s^1, t_o^1)$ un état tel que $m_1 = \{(s_1, o_1, \text{read}), (s_1, o_2, \text{read})\}$, $t_s^1(s_1) = \{t_1, t_2\}$, $t_s^1(s_2) = \{t_2\}$, $t_o^1(o_1) = t_o^1(o_2) = t_o^1(o_3) = \{t_1\}$ et $t_o^1(o_4) = \{t_1, t_2\}$. On constate qu'il n'est pas possible d'ajouter à σ_1 un ensemble d'accès contenant $\{(s_1, o_3, \text{read}), (s_1, o_4, \text{read})\}$, car dans ce cas, s_1 accéderait à plus de trois ressources en même temps et cet état ne respecterait alors pas le prédicat Ω_e . De même, on ne peut pas ajouter un ensemble d'accès où s_2 accéderait à o_1 , o_2 ou o_3 , car s_2 n'appartient pas à l'équipe t_1 , et seuls les membres de cette équipe peuvent accéder à o_1 , o_2 ou o_3 . On a donc :

$$\mathcal{W}(\sigma_1) = \left\{ A \in \wp(\mathcal{S}'_e \times \mathcal{O}'_e \times \mathcal{A}'_e) \mid \right. \\ \left. \begin{aligned} &\{(s_1, o_3, \text{read}), (s_1, o_4, \text{read})\} \not\subseteq A \wedge (s_2, o_1, \text{read}) \notin A \\ &\wedge (s_2, o_2, \text{read}) \notin A \wedge (s_2, o_3, \text{read}) \notin A \end{aligned} \right\}$$

On introduit également la fonction $\mathcal{W}_\emptyset : \Sigma \rightarrow \wp(\wp(\mathbb{A}))$, qui étant donné un état, retourne tous les ensembles d'accès « compatibles » avec les fonctions de sécurité de cet état. Etant donné un état σ , $\mathcal{W}_\emptyset(\sigma) = \mathcal{W}(\sigma')$ avec $\Lambda(\sigma') = \emptyset$ et $\Upsilon(\sigma') = \Upsilon(\sigma)$. Ces définitions permettent d'établir plusieurs propriétés « techniques » utiles lors de la comparaison de politiques de contrôle d'accès. On peut montrer par exemple que si un état σ est tel que $\mathcal{W}(\sigma) = \emptyset$, alors il n'est pas sûr (*i.e.* $\Omega(\sigma)$ est faux). La réciproque n'est cependant pas vraie dans le cas général mais seulement pour les politiques pour lesquelles enlever des accès dans un état sûr n'entraîne pas une violation de la politique de sécurité. Nous appelons politiques compactes les politiques vérifiant cette propriété.

Définition 3 Une politique $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$ est compacte ssi :

$$\forall \sigma_1 \in \Sigma \quad \Omega(\sigma_1) \Rightarrow (\forall \sigma_2 \in \Sigma \quad (\Lambda(\sigma_2) \subseteq \Lambda(\sigma_1) \wedge \Upsilon(\sigma_1) = \Upsilon(\sigma_2)) \Rightarrow \Omega(\sigma_2))$$

Il est alors possible de montrer qu'une politique $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$ est compacte ssi, pour tout état σ , $\neg\Omega(\sigma) \Rightarrow \mathcal{W}(\sigma) = \emptyset$.

EXEMPLE (SUITE). La politique $\mathbb{P}_e[\rho_e] = (\mathcal{S}_e, \mathcal{O}_e, \mathcal{A}_e, \Sigma_e, \Omega_e)$ est compacte car pour chaque état sûr, il est possible d'enlever des accès tout en préservant la propriété exprimée par le prédicat Ω_e . En revanche, considérons le cas où un utilisateur est autorisé à utiliser des ressources d'une équipe à laquelle il n'appartient pas, mais seulement dans le cas où toutes les ressources de son équipe sont déjà accédées. Une telle politique, définie par un prédicat noté Ω'_e , n'est pas compacte puisque lorsqu'un sujet accède à une ressource d'une équipe à laquelle il n'appartient pas, retirer un accès à une ressource de son équipe conduit à un état non sûr.

D'un point de vue formel, le fait qu'une politique soit compacte permet de garantir un certain nombre de propriétés, que nous ne détaillons pas ici, mais qui prennent toute leur importance dans les preuves de certains résultats, notamment lors des preuves de correction des implantations d'un modèle (section 2.2.2.1). D'un point de vue plus pratique, le caractère compact d'une politique peut permettre de simplifier le traitement des accès présents. Par exemple, si l'on souhaite supprimer (ou désactiver) un utilisateur du système, il faut également supprimer tous les accès en cours effectués par cet utilisateur. Si la politique est compacte, alors on a la garantie qu'enlever tous ces accès n'entraînera pas une violation de la politique de sécurité.

2.2. Modèles de contrôle d'accès

Nous introduisons à présent la notion de modèle de contrôle d'accès, qui permet de spécifier comment passer d'un état du système à un autre. Pour cela, nous introduisons tout d'abord la notion de requête, puis celle d'implantation.

2.2.1. Requêtes

Une requête est généralement soumise par un sujet afin de faire évoluer le système, soit en ajoutant ou en enlevant un accès, soit en changeant les informations du système. La plupart des modèles de contrôle d'accès considèrent au moins les droits d'accès **read** (lecture) et **write** (écriture). On peut généralement considérer les requêtes suivantes :

- le sujet s demande la permission de lire (resp. d'écrire) un objet o . On note $\langle +, s, o, \text{read} \rangle$ (resp. $\langle +, s, o, \text{write} \rangle$) une telle requête ;
- le sujet s demande de relâcher l'accès en lecture (resp. en écriture) sur un objet o . On note $\langle -, s, o, \text{read} \rangle$ (resp. $\langle -, s, o, \text{write} \rangle$) une telle requête.

La notion de relâchement d'accès n'est pas nécessairement présente dans tous les modèles de contrôle d'accès. En effet, elle sous-entend la notion (implicite) de persistance des accès, c'est-à-dire qu'une fois qu'ils sont effectués, ils restent en mémoire.

Il est possible d'introduire une notion de sémantique des requêtes, correspondant à une « sémantique de transitions », en définissant une relation $\llbracket \mathcal{R} \rrbracket_{\Sigma}^+ \subseteq \Sigma \times \mathcal{R} \times \Sigma$. Avec une telle approche, $(\sigma_1, R, \sigma_2) \in \llbracket \mathcal{R} \rrbracket_{\Sigma}^+$ permet de spécifier les propriétés d'un état σ_2 lorsqu'il a été obtenu par application d'une requête R sur un état σ_1 . Toutefois,

nous n'adoptons pas ici une telle approche. Nous nous contentons d'une sémantique « faible » définie par une relation $\|\mathcal{R}\|_{\Sigma} \subseteq \mathcal{R} \times \Sigma$ telle que (R, σ) appartient à $\|\mathcal{R}\|_{\Sigma}$, si l'état σ a pu être obtenu en appliquant avec succès la requête R (on ne tient pas compte de l'état de départ). Par exemple, une sémantique faible possible pour l'ensemble \mathcal{R} contenant les requêtes décrites plus haut est :

$$\begin{aligned} \langle \langle +, s, o, x \rangle, \sigma \rangle \in \|\mathcal{R}\|_{\Sigma} &\Leftrightarrow (s, o, x) \in \Lambda(\sigma) \\ \langle \langle -, s, o, x \rangle, \sigma \rangle \in \|\mathcal{R}\|_{\Sigma} &\Leftrightarrow (s, o, x) \notin \Lambda(\sigma) \quad \text{où } x \in \{\text{read}, \text{write}\} \end{aligned}$$

La notion de sémantique faible des requêtes que nous venons d'introduire peut être considérée comme « atomique », dans le sens où elle spécifie les propriétés que doit vérifier un état après application d'une requête, et non pas les changements effectués à partir d'un état. Néanmoins, ces changements sont en partie caractérisés par la partition des requêtes, que nous introduisons ci-après. En effet, nous introduisons la partition suivante de l'ensemble \mathcal{R} :

$$\mathcal{R} = \mathcal{R}^{\otimes} \cup \mathcal{R}^{\ominus} \cup \mathcal{R}^{\oplus}$$

qui permet de spécifier la variation des accès potentiels lors de l'application des requêtes. L'ensemble \mathcal{R}^{\otimes} (resp. \mathcal{R}^{\ominus}) contient les requêtes d'élargissement (resp. rétrécissement) des accès potentiels et l'ensemble \mathcal{R}^{\oplus} contient les autres requêtes. Autrement dit, si l'on passe d'un état σ_1 à un état σ_2 en appliquant avec succès une requête $R \in \mathcal{R}^{\otimes}$ (resp. $R \in \mathcal{R}^{\ominus}$), alors l'ensemble des ensembles d'accès que l'on peut ajouter à σ_2 (resp. σ_1), sans modifier les fonctions de sécurité, est inclus dans celui des ensembles d'accès que l'on peut ajouter à σ_1 (resp. σ_2) sans modifier les fonctions de sécurité. L'utilité de cette partition sera visible par la suite, lorsque nous considèrerons les implantations d'une politique de contrôle d'accès, et en particulier celles dites \mathcal{W} -conformes, notion introduite formellement en (1).

EXEMPLE (SUITE). Si l'on considère la politique $\mathbb{P}_e[\rho_e] = (\mathcal{S}_e, \mathcal{O}_e, \mathcal{A}_e, \Sigma_e, \Omega_e)$, on peut définir la partition suivante :

$$\begin{aligned} \mathcal{R}^{\otimes} &= \{ \langle -, s, o, \text{read} \rangle, \langle -, s, o, \text{write} \rangle, \langle +, s, t \rangle \} \\ \mathcal{R}^{\ominus} &= \{ \langle +, s, o, \text{read} \rangle, \langle +, s, o, \text{write} \rangle, \langle -, s, t \rangle \} \end{aligned} \quad \mathcal{R}^{\oplus} = \emptyset$$

En effet, enlever un accès ou rajouter une équipe à un utilisateur permet par la suite d'effectuer *a priori* plus d'accès. De même, ajouter un accès ou enlever une équipe à un utilisateur permet par la suite d'effectuer *a priori* moins d'accès. En revanche, avec la politique $\mathbb{P}_e[\rho_e] = (\mathcal{S}_e, \mathcal{O}_e, \mathcal{A}_e, \Sigma_e, \Omega'_e)$, qui, rappelons le, permet à un utilisateur d'accéder à des ressources d'autres équipes que les siennes à la condition que toutes les ressources de ses équipes soient déjà accédées, la partition des requêtes est différente. En effet, enlever un accès permet de faire moins d'accès, puisque cela prive potentiellement un utilisateur d'accéder à des ressources qui n'appartiennent pas à ses équipes. De même ajouter un accès permet d'effectuer éventuellement plus d'accès, car toutes les ressources des équipes d'un utilisateur peuvent être ainsi accédées, autorisant ce dernier à accéder à des ressources d'autres équipes. L'ajout ou le retrait d'équipes pour un utilisateur est plus complexe. En effet, considérons par exemple le

cas où un utilisateur s_1 appartient uniquement à l'équipe t_1 et où toutes les ressources de t_1 sont déjà accédées. Le sujet s_1 peut alors accéder à des ressources des autres équipes, par exemple t_2 et t_3 . Si on ajoute l'équipe t_2 à s_1 et qu'il existe des ressources non accédées de t_2 , s_1 ne peut plus accéder aux ressources de t_3 . Dans ce cas, ajouter une équipe à un utilisateur permet d'effectuer moins d'accès. Si en revanche toutes les ressources de t_1 ne sont pas déjà accédées, alors s_1 ne peut pas accéder aux ressources de t_2 et t_3 . Ajouter l'équipe t_2 à s_1 permet dans ce cas à ce dernier d'accéder aux ressources de t_2 , et donc d'une manière générale, d'effectuer plus d'accès. L'ajout d'une équipe à un utilisateur permet donc d'effectuer plus d'accès dans certains cas et d'en effectuer moins dans d'autres cas. Le retrait d'une équipe d'un utilisateur étant similaire, les requêtes d'ajout ou de retrait d'équipes sont ainsi classées dans les requêtes de « maintenance ». On obtient alors la partition suivante :

$$\begin{aligned} \mathcal{R}^{\ominus} &= \{ \langle +, s, o, \text{read} \rangle, \langle +, s, o, \text{write} \rangle \} \\ \mathcal{R}^{\oplus} &= \{ \langle -, s, o, \text{read} \rangle, \langle -, s, o, \text{write} \rangle \} \end{aligned} \quad \mathcal{R}^{\circ} = \{ \langle +, s, t \rangle, \langle -, s, t \rangle \}$$

2.2.2. Modèles et implantations

2.2.2.1. Définitions et propriétés

La notion de modèle est définie comme suit.

Définition 4 (Modèle de contrôle d'accès) *Etant donné un paramètre de sécurité ρ , un modèle de contrôle d'accès $\mathbb{M}[\rho]$ est défini par une paire $\mathbb{M}[\rho] = (\mathbb{P}[\rho], \llbracket \mathcal{R} \rrbracket_{\Sigma})$ où $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$ est une politique de contrôle d'accès, $\mathcal{R} = \mathcal{R}^{\ominus} \cup \mathcal{R}^{\oplus} \cup \mathcal{R}^{\circ}$ est un ensemble de requêtes, et $\llbracket \mathcal{R} \rrbracket_{\Sigma} \subseteq \mathcal{R} \times \Sigma$ est une relation spécifiant la sémantique faible des requêtes.*

L'implantation d'un modèle de contrôle d'accès $\mathbb{M}[\rho]$ sous la forme d'une machine à états consiste à définir à la fois un ensemble d'états initiaux Σ_I et une fonction de transition τ qui permet de passer d'un état à un autre en fonction d'une requête.

Définition 5 (Implantation) *Une implantation d'un modèle de contrôle d'accès $\mathbb{M}[\rho] = (\mathbb{P}[\rho], \llbracket \mathcal{R} \rrbracket_{\Sigma})$ basé sur une politique $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$ est une paire (τ, Σ_I) où Σ_I est un ensemble d'états initiaux, $\tau : \mathcal{R} \times \Sigma \rightarrow \mathcal{D} \times \Sigma$ est une fonction de transition, et $\mathcal{D} = \{\text{yes}, \text{no}\}$ est un ensemble de réponses.*

On note $\Gamma_{\tau}(E)$ l'ensemble des états du système atteignables à partir d'un état appartenant à l'ensemble E en appliquant un nombre fini de fois la fonction τ . Nous pouvons à présent définir certaines propriétés sur les implantations d'un modèle.

- L'implantation (τ, Σ_I) est dite $\mathbb{P}[\rho]$ -correcte ssi tout état atteignable est sûr :

$$\mathbb{P}[\rho] \vdash (\tau, \Sigma_I) \Leftrightarrow \Gamma_{\tau}(\Sigma_I) \subseteq \Sigma_{|\Omega}$$

– La fonction de transition $\tau : \mathcal{R} \times \Sigma \rightarrow \mathcal{D} \times \Sigma$ est dite \mathcal{W} -conforme⁴ ssi :

$$\begin{aligned} & \forall \sigma_1, \sigma_2 \in \Sigma \forall d \in \mathcal{D} \forall R \in \mathcal{R} \\ & \tau(R, \sigma_1) = (d, \sigma_2) \Rightarrow \\ & \left(\begin{array}{l} d = \text{yes} \Rightarrow \left(\begin{array}{l} R \in \mathcal{R}^\otimes \Rightarrow \mathcal{W}(\sigma_1) \subseteq \mathcal{W}(\sigma_2) \\ \wedge R \in \mathcal{R}^\otimes \Rightarrow \mathcal{W}(\sigma_2) \subseteq \mathcal{W}(\sigma_1) \end{array} \right) \\ \wedge d = \text{no} \Rightarrow \mathcal{W}(\sigma_2) \subseteq \mathcal{W}(\sigma_1) \end{array} \right) \end{array} \quad [1] \end{aligned}$$

– La fonction de transition τ est dite \mathcal{R} -correcte selon $\|\mathcal{R}\|_\Sigma$, ce qui est noté $\|\mathcal{R}\|_\Sigma \vdash \tau$ ssi :

$$\forall \sigma_1, \sigma_2 \in \Sigma \forall R \in \mathcal{R} \quad \tau(R, \sigma_1) = (\text{yes}, \sigma_2) \Rightarrow (R, \sigma_2) \in \|\mathcal{R}\|_\Sigma$$

– Etant donné un modèle de contrôle d'accès $\mathbb{M}[\rho] = (\mathbb{P}[\rho], \|\mathcal{R}\|_\Sigma)$, l'implantation (τ, Σ_I) est dite $\mathbb{M}[\rho]$ -correcte ssi elle est $\mathbb{P}[\rho]$ -correcte, $\|\mathcal{R}\|_\Sigma$ -correcte et \mathcal{W} -conforme. ce que nous notons $\mathbb{M}[\rho] \vdash (\tau, \Sigma_I)$.

De plus, comme nous le verrons par la suite, il est parfois utile de considérer les fonctions de transition qui « préservent » une certaine relation d'équivalence, c'est-à-dire les fonctions qui appliquées à deux états équivalents renvoient la même réponse et deux états encore équivalents. Plus formellement, une fonction de transition τ est dite \equiv -préservante, ce que l'on note $\equiv \vdash \tau$, ssi :

$$\begin{aligned} & \forall \sigma_1, \sigma_2, \sigma'_1, \sigma'_2 \in \Sigma \forall R \in \mathcal{R} \forall d \in \mathcal{D} \\ & \left(\begin{array}{l} \sigma_1 \equiv \sigma_2 \\ \wedge \tau(R, \sigma_1) = (d_1, \sigma'_1) \wedge \tau(R, \sigma_2) = (d_2, \sigma'_2) \end{array} \right) \Rightarrow \left(\begin{array}{l} \sigma'_1 \equiv \sigma'_2 \\ \wedge d_1 = d_2 \end{array} \right) \end{aligned}$$

2.2.2.2. Préordre sur les implantations

Etant donné un modèle, plusieurs implantations « correctes », plus ou moins restrictives, de ce modèle peuvent être envisagées. Ces implantations peuvent correspondre à différents modes de fonctionnement du système. Nous introduisons à présent une notion de préordre sur les implantations d'un même modèle de contrôle d'accès. Nous définissons tout d'abord le préordre \sqsubseteq_Γ exprimant qu'une implantation (τ_1, Σ_I^1) est plus restrictive en termes d'états atteignables qu'une implantation (τ_2, Σ_I^2) ssi tout état atteignable par (τ_1, Σ_I^1) l'est également par (τ_2, Σ_I^2) . Nous introduisons ensuite le préordre $\sqsubseteq_{\mathcal{W}}$ sur les fonctions de transitions. Intuitivement, $\tau_1 \sqsubseteq_{\mathcal{W}} \tau_2$ signifie que τ_2 permet de faire des « plus petits pas » que τ_1 . En d'autres termes, si τ_1 permet d'atteindre un état σ_1 à partir d'un état σ , alors σ_1 est également atteignable par τ_2 à partir d'un état σ_2 qui est « plus proche » de σ que σ_1 . La figure 1 illustre ce préordre pour des fonctions \mathcal{W} -conformes.

4. Dans le cas où la réponse est **no**, la fonction de transition peut renvoyer un état différent. C'est le cas par exemple des distributeurs de billets qui, lorsque le code saisi par l'utilisateur est faux, refusent la transaction et modifie l'état du système afin de compter le nombre de tentatives de saisie du code.

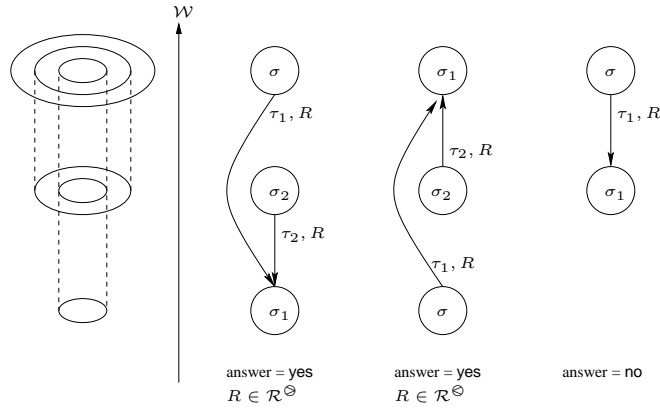


Figure 1. Préordre sur les fonctions \mathcal{W} -conformes

Définition 6

$$-(\tau_1, \Sigma_I^1) \sqsubseteq_{\Gamma} (\tau_2, \Sigma_I^2) \Leftrightarrow \Gamma_{\tau_1}(\Sigma_I^1) \subseteq \Gamma_{\tau_2}(\Sigma_I^2)$$

– Etant donné deux fonctions de transition τ_1 et τ_2 de $\mathcal{R} \times \Sigma$ vers $\mathcal{D} \times \Sigma$, $\tau_1 \sqsubseteq_{\mathcal{W}} \tau_2$ ssi :

$$\begin{aligned} & \forall \sigma, \sigma_1 \in \Sigma \forall R \in \mathcal{R} \\ & \tau_1(R, \sigma) = (\text{yes}, \sigma_1) \\ & \Rightarrow \left(\begin{array}{l} \exists \sigma_2 \in \Sigma \quad \tau_2(R, \sigma_2) = (\text{yes}, \sigma_1) \\ \wedge \quad R \in \mathcal{R}^{\ominus} \Rightarrow \mathcal{W}(\sigma_2) \subseteq \mathcal{W}(\sigma) \\ \wedge \quad R \in \mathcal{R}^{\ominus} \Rightarrow \mathcal{W}(\sigma) \subseteq \mathcal{W}(\sigma_2) \end{array} \right) \\ & \wedge \quad \tau_1(R, \sigma) = (\text{no}, \sigma_1) \Rightarrow \mathcal{W}(\sigma_1) \subseteq \mathcal{W}(\sigma) \end{aligned}$$

– La relation de préordre sur les implantations d’un modèle est définie par :

$$(\tau_1, \Sigma_I^1) \sqsubseteq (\tau_2, \Sigma_I^2) \Leftrightarrow ((\tau_1, \Sigma_I^1) \sqsubseteq_{\Gamma} (\tau_2, \Sigma_I^2) \wedge \tau_1 \sqsubseteq_{\mathcal{W}} \tau_2)$$

On peut alors prouver que toute implantation inférieure (selon \sqsubseteq) à une implantation « correcte » est elle-même « correcte ». Ce résultat sera utile lorsque nous envisagerons la comparaison de modèles de contrôle d’accès.

Lemme 1 Soit $\mathbb{M}[\rho] = (\mathbb{P}[\rho], \|\mathcal{R}\|_{\Sigma})$ un modèle de contrôle d’accès basé sur une politique $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$, et (τ_1, Σ_I^1) et (τ_2, Σ_I^2) deux implantations de $\mathbb{M}[\rho]$. Si $(\tau_1, \Sigma_I^1) \sqsubseteq (\tau_2, \Sigma_I^2)$ et $\mathbb{M}[\rho] \vdash (\tau_2, \Sigma_I^2)$ alors $\mathbb{M}[\rho] \vdash (\tau_1, \Sigma_I^1)$.

2.2.2.3. Modèles réduits

Il est parfois utile de définir une relation sur l’ensemble des états définis par une politique de sécurité permettant de caractériser les états équivalents pour le modèle

de contrôle d'accès considéré. Considérons par exemple le cas où une fonction de sécurité d'un état permet d'obtenir l'heure courante, afin de pouvoir enregistrer dans des fichiers de « logs » chaque action effectuée ainsi que l'heure à laquelle elle a été effectuée. L'heure de l'accès est une information qui n'a aucun impact sur la politique de sécurité ou le modèle. Autrement dit, une requête est autorisée ou non indépendamment de l'heure. Dans ce cas, deux états contenant les mêmes accès et les mêmes informations de sécurité, mais deux heures différentes, peuvent être considérés comme équivalents. Nous reviendrons par la suite de manière plus formelle sur cette notion d'équivalence entre états. Nous introduisons ici la notion de modèles réduits, qui consiste essentiellement à considérer les classes d'équivalence d'états plutôt que les états. Etant donnée une relation d'équivalence \equiv sur les états et un état σ , $[\sigma]$ représente la classe d'équivalence de σ et Σ/\equiv représente l'ensemble quotient par rapport à \equiv de Σ . De plus, nous notons $e(\sigma)$ l'élément canonique associé à σ lorsque la relation d'équivalence est définie conjointement avec une fonction de projection $e : \Sigma \rightarrow \Sigma$ telle que :

$$\forall \sigma, \sigma' \in \Sigma \quad \sigma \equiv \sigma' \Leftrightarrow e(\sigma) = e(\sigma')$$

Etant donné un ensemble E d'états, nous notons $\hat{e}(E) = \{e(\sigma) \mid \sigma \in E\}$.

Définition 7 Soit $\mathbb{P}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma, \Omega)$ une politique de contrôle d'accès, $\mathbb{M}[\rho] = (\mathbb{P}[\rho], \|\mathcal{R}\|_{\Sigma})$ un modèle de contrôle d'accès et \equiv une relation d'équivalence sur Σ définie conjointement avec une fonction de projection $e : \Sigma \rightarrow \Sigma$ telle que :

$$\begin{aligned} (\sigma_1 \equiv \sigma_2 \wedge \Omega(\sigma_1)) &\Rightarrow \Omega(\sigma_2) \\ \forall R \in \mathcal{R} \quad (\sigma_1 \equiv \sigma_2 \wedge (R, \sigma_1) \in \|\mathcal{R}\|_{\Sigma}) &\Rightarrow (R, \sigma_2) \in \|\mathcal{R}\|_{\Sigma} \end{aligned}$$

– La réduction de la politique $\mathbb{P}[\rho]$ selon la relation d'équivalence \equiv est la politique $\mathbb{P}_{\equiv}^{\#}[\rho] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \hat{e}(\Sigma), \Omega)$.

– La réduction du modèle $\mathbb{M}[\rho]$ selon la relation d'équivalence \equiv est le modèle $\mathbb{M}_{\equiv}^{\#}[\rho] = (\mathbb{P}_{\equiv}^{\#}[\rho], \|\mathcal{R}\|_{\hat{e}(\Sigma)})$ où $\|\mathcal{R}\|_{\hat{e}(\Sigma)} = \{(R, \sigma) \in \|\mathcal{R}\|_{\Sigma} \mid \sigma \in \hat{e}(\Sigma)\}$.

Parmi les différentes relations d'équivalence possibles pour envisager la réduction d'un modèle de contrôle d'accès, on peut en distinguer plusieurs.

Définition 8 Soit $\mathbb{M}[\rho] = (\mathbb{P}[\rho], \|\mathcal{R}\|_{\Sigma})$ un modèle de contrôle d'accès.

- $\sigma_1 \equiv_{\mathcal{W}} \sigma_2 \Leftrightarrow \mathcal{W}(\sigma_1) = \mathcal{W}(\sigma_2)$
- $\sigma_1 \equiv_{\mathcal{W}_0} \sigma_2 \Leftrightarrow \mathcal{W}_0(\sigma_1) = \mathcal{W}_0(\sigma_2)$
- $\sigma_1 \equiv_{\mathcal{R}} \sigma_2 \Leftrightarrow (\forall R \in \mathcal{R} \quad (\sigma_1, R) \in \|\mathcal{R}\|_{\Sigma} \Leftrightarrow (\sigma_2, R) \in \|\mathcal{R}\|_{\Sigma})$
- $\equiv_l = (\equiv_{\mathcal{W}} \cap \equiv_{\mathcal{W}_0} \cap \equiv_{\mathcal{R}})$

Intuitivement, deux états sont équivalents par \equiv_l ssi ils ont le même passé (ils ont pu être construits à partir des mêmes requêtes et leurs fonctions de sécurité permettent

les mêmes ensembles d'accès) et le même futur (ils autorisent les mêmes ensembles d'accès).

EXEMPLE (SUITE). Considérons les ensembles restreints de sujets $\mathcal{S}_e'' = \{s_1, s_2, s_3\}$, d'objets $\mathcal{O}_e'' = \{o_1, o_2\}$ et de noms d'équipes $\rho_e'' = \{t_A, t_B\}$. Les deux états $\sigma_1 = (\emptyset, t_s^1, t_o^1)$ et $\sigma_2 = (\emptyset, t_s^2, t_o^2)$ avec :

$$\begin{aligned} t_s^1(s_1) &= t_s^1(s_2) = t_A & t_s^1(s_3) &= t_B & t_o^1(o_1) &= t_A & t_o^1(o_2) &= t_B \\ t_s^2(s_1) &= t_s^2(s_2) = t_B & t_s^2(s_3) &= t_A & t_o^2(o_1) &= t_B & t_o^2(o_2) &= t_A \end{aligned}$$

sont différents mais équivalents selon \equiv_ι .

On montre facilement que la relation d'équivalence \equiv_ι permet de construire des modèles réduits, car elle vérifie les propriétés requises. Ici nous considérons principalement des réductions selon la relation d'équivalence \equiv_ι , bien que certains des résultats obtenus puissent être généralisés à d'autres relations d'équivalence. Etant donné une politique $\mathbb{P}[\rho]$ (resp. un modèle $\mathbb{M}[\rho]$), nous notons simplement $\mathbb{P}^\sharp[\rho]$ la politique $\mathbb{P}^\sharp_{\equiv_\iota}[\rho]$ (resp. $\mathbb{M}^\sharp[\rho]$ le modèle $\mathbb{M}^\sharp_{\equiv_\iota}[\rho]$) afin d'alléger les notations.

Etant donné un modèle $\mathbb{M}[\rho]$ et le modèle réduit associé $\mathbb{M}^\sharp[\rho]$, les implantations du premier peuvent être reliées aux implantations du deuxième, et inversement. En effet, pour toute implantation de $\mathbb{M}[\rho]$, il est possible de construire une implantation de $\mathbb{M}^\sharp[\rho]$ à l'aide de l'opérateur :

$$\begin{aligned} \sharp : (\mathcal{R} \times \Sigma \rightarrow \mathcal{D} \times \Sigma) &\rightarrow (\mathcal{R} \times \hat{e}(\Sigma) \rightarrow \mathcal{D} \times \hat{e}(\Sigma)) \\ \forall \sigma \in \hat{e}(\Sigma) \forall R \in \mathcal{R} &\quad \sharp(\tau)(R, \sigma) = (d, e(\sigma')) \quad \text{avec} \quad \tau(R, \sigma) = (d, \sigma') \end{aligned}$$

Réciproquement, pour toute implantation de $\mathbb{M}^\sharp[\rho]$, il est possible de construire une implantation de $\mathbb{M}[\rho]$ à l'aide de l'opérateur :

$$\begin{aligned} \flat : (\mathcal{R} \times \hat{e}(\Sigma) \rightarrow \mathcal{D} \times \hat{e}(\Sigma)) &\rightarrow (\mathcal{R} \times \Sigma \rightarrow \mathcal{D} \times \Sigma) \\ \forall \sigma \in \Sigma \forall R \in \mathcal{R} &\quad \flat(\tau)(R, \sigma) = \tau(R, e(\sigma)) \end{aligned}$$

On montre que les opérateurs \sharp et \flat , lorsqu'ils sont appliqués à des implantations « correctes », permettent d'obtenir des implantations « correctes ».

Lemme 2 Soit $\mathbb{M}[\rho]$ un modèle et $\mathbb{M}^\sharp[\rho]$ la réduction de ce modèle selon la relation d'équivalence (\equiv_ι, e) .

- 1) $\mathbb{M}^\sharp[\rho] \vdash (\tau, \Sigma_I) \Rightarrow (\mathbb{M}[\rho] \vdash (\flat(\tau), \Sigma_I) \wedge \equiv_\iota \vdash \flat(\tau))$
- 2) $(\mathbb{M}[\rho] \vdash (\tau, \Sigma_I) \wedge \equiv_\iota \vdash \tau) \Rightarrow \mathbb{M}^\sharp[\rho] \vdash (\sharp(\tau), \hat{e}(\Sigma_I))$

On montre par ailleurs que l'opérateur \sharp est monotone pour le préordre sur les implantations. La notion de réduction de modèles permet d'abstraire un modèle en regroupant les états équivalents selon une certaine sémantique définie par la relation d'équivalence utilisée pour construire le modèle réduit. Notons cependant qu'en pratique, un modèle réduit n'a pas vocation à être effectivement construit (*i.e.* calculé par un algorithme). En effet, comme on le verra, la notion de modèle réduit sert essentiellement

à simplifier certaines preuves (en faisant abstraction d'informations « non discriminantes » au regard de la politique). Comparer deux modèles de contrôle d'accès ne nécessite pas forcément de les réduire (on peut par exemple utiliser le théorème 3 dont l'énoncé ne fait pas intervenir la notion de modèles réduits, bien que sa preuve repose fortement sur cette notion). Toutefois, la caractérisation du modèle réduit associé à un modèle permet de simplifier sa manipulation dans les raisonnements et d'en avoir une compréhension plus fine.

3. Comparaison de modèles de contrôle d'accès

3.1. Préordre sur les modèles de contrôle d'accès

Il est maintenant possible de comparer deux modèles de contrôle d'accès. Intuitivement, le préordre sur les modèles que nous introduisons permet de dire qu'un modèle $\mathbb{M}_1[\rho_1]$ est plus restrictif qu'un modèle $\mathbb{M}_2[\rho_2]$ ssi toute implantation correcte de $\mathbb{M}_1[\rho_1]$ peut être simulée par une implantation correcte de $\mathbb{M}_2[\rho_2]$.

Il nous faut donc tout d'abord introduire les notions classiques relatives à la simulation d'implantations. Etant donné deux fonctions de transition $\tau_1 : \mathcal{R} \times \Sigma_1 \rightarrow \mathcal{D} \times \Sigma_1$ et $\tau_2 : \mathcal{R} \times \Sigma_2 \rightarrow \mathcal{D} \times \Sigma_2$, τ_2 simule τ_1 , ce que nous notons $\tau_1 \stackrel{\kappa_\Sigma}{\sim} \tau_2$, ssi il existe une relation $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ telle que :

$$\begin{aligned} & \forall \sigma_1, \sigma'_1 \in \Sigma_1 \quad \forall \sigma_2 \in \Sigma_2 \quad \forall R \in \mathcal{R} \quad \forall a \in \mathcal{D} \\ & \quad ((\sigma_1, \sigma_2) \in \kappa_\Sigma \wedge \tau_1(R, \sigma_1) = (a, \sigma'_1)) \\ & \Rightarrow \quad (\exists \sigma'_2 \in \Sigma_2 \quad (\sigma'_1, \sigma'_2) \in \kappa_\Sigma \wedge \tau_2(R, \sigma_2) = (a, \sigma'_2)) \end{aligned}$$

On étend cette définition aux implantations : l'implantation (τ_2, Σ_2^2) simule l'implantation (τ_1, Σ_1^1) , ce que nous notons $(\tau_1, \Sigma_1^1) \stackrel{\kappa_\Sigma}{\sim} (\tau_2, \Sigma_2^2)$, ssi il existe une relation $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ telle que :

$$\tau_1 \stackrel{\kappa_\Sigma}{\sim} \tau_2 \wedge \forall \sigma_1 \in \Sigma_1^1 \quad \exists \sigma_2 \in \Sigma_2^2 \quad (\sigma_1, \sigma_2) \in \kappa_\Sigma$$

En fait, il est nécessaire de préciser la notion d'ordre entre modèles. En effet, la relation de simulation utilisée pour montrer qu'un modèle $\mathbb{M}_1[\rho_1]$ est plus restrictif qu'un modèle $\mathbb{M}_2[\rho_2]$ doit satisfaire de « bonnes propriétés ». Par exemple, si on considère le produit cartésien $\Sigma_1 \times \Sigma_2$ comme une relation de simulation entre implantations, il devient facile d'établir que tout modèle est plus restrictif que tout autre modèle. Il faut donc contraindre la notion de relation de simulation comme suit. Il faut tout d'abord que tout état $\sigma_1 \in \Sigma_1$ soit en relation avec un état $\sigma_2 \in \Sigma_2$. La relation κ_Σ doit donc être totale à gauche⁵. En effet, intuitivement, $\mathbb{M}_1[\rho_1]$ est plus restrictif que $\mathbb{M}_2[\rho_2]$ ssi tout ce qui peut être fait avec $\mathbb{M}_1[\rho_1]$ peut également l'être avec $\mathbb{M}_2[\rho_2]$, donc il faut au moins que tous les états de Σ_1 soient en relation avec des

5. Une relation $R \subseteq X \times Y$ est dite totale à gauche ssi pour tout x dans X il existe un y dans Y tel que $(x, y) \in R$.

états de Σ_2 . Une autre contrainte consiste à imposer que deux états de Σ_1 équivalents selon \equiv_{ι_1} , soient en relation avec des états de Σ_2 équivalents selon \equiv_{ι_2} et *vice-versa*. Intuitivement, deux états sont reliés s'il est possible de « faire les mêmes choses » à partir de ces deux états. Nous introduisons donc les deux notions suivantes :

– $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ est dite ι -fonctionnelle ssi :

$$\begin{aligned} & \forall \sigma_1, \sigma'_1 \in \Sigma_1 \quad \forall \sigma_2, \sigma'_2 \in \Sigma_2 \\ & \sigma_1 \equiv_{\iota_1} \sigma'_1 \wedge (\sigma_1, \sigma_2) \in \kappa_\Sigma \wedge (\sigma'_1, \sigma'_2) \in \kappa_\Sigma \Rightarrow \sigma_2 \equiv_{\iota_2} \sigma'_2 \end{aligned}$$

– $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ est dite ι -injective ssi :

$$\begin{aligned} & \forall \sigma_1, \sigma'_1 \in \Sigma_1 \quad \forall \sigma_2, \sigma'_2 \in \Sigma_2 \\ & \sigma_2 \equiv_{\iota_2} \sigma'_2 \wedge (\sigma_1, \sigma_2) \in \kappa_\Sigma \wedge (\sigma'_1, \sigma'_2) \in \kappa_\Sigma \Rightarrow \sigma_1 \equiv_{\iota_1} \sigma'_1 \end{aligned}$$

Notons que si pour les deux modèles, la relation \equiv_{ι} est l'égalité, alors la ι -fonctionnalité correspond intuitivement à la notion de fonctionnalité⁶, et la ι -injectivité à la notion d'injectivité⁷. On peut à présent exprimer de manière formelle qu'un modèle de contrôle d'accès $\mathbb{M}_1[\rho_1]$ est plus restrictif qu'un modèle $\mathbb{M}_2[\rho_2]$.

Définition 9 (Préordre sur les modèles) *Etant donné deux modèles de contrôle d'accès $\mathbb{M}_1[\rho_1] = (\mathbb{P}_1[\rho_1], \|\mathcal{R}\|_{\Sigma_1})$ et $\mathbb{M}_2[\rho_2] = (\mathbb{P}_2[\rho_2], \|\mathcal{R}\|_{\Sigma_2})$ basés respectivement sur les politiques $\mathbb{P}_1[\rho_1] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_1, \Omega_1)$ et $\mathbb{P}_2[\rho_2] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_2, \Omega_2)$, $\mathbb{M}_1[\rho_1]$ est plus restrictif que $\mathbb{M}_2[\rho_2]$, ce que nous notons $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$, ssi il existe une relation $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ totale à gauche, ι -fonctionnelle et ι -injective telle que :*

$$\begin{aligned} & \forall \tau_1 : \mathcal{R} \times \Sigma_1 \rightarrow \mathcal{D} \times \Sigma_1 \quad \forall \Sigma_I^1 \subseteq \Sigma_1 \\ & \mathbb{M}_1[\rho_1] \vdash (\tau_1, \Sigma_I^1) \wedge \equiv_{\iota_1} \vdash \tau_1 \\ \Rightarrow & \exists \tau_2 : \mathcal{R} \times \Sigma_2 \rightarrow \mathcal{D} \times \Sigma_2 \quad \exists \Sigma_I^2 \subseteq \Sigma_2 \\ & \mathbb{M}_2[\rho_2] \vdash (\tau_2, \Sigma_I^2) \wedge \equiv_{\iota_2} \vdash \tau_2 \wedge (\tau_1, \Sigma_I^1) \stackrel{\kappa_\Sigma}{\sim} (\tau_2, \Sigma_I^2) \end{aligned}$$

3.2. Préordre sur les modèles réduits

La relation de préordre sur les modèles définie précédemment est relativement dépendante de la relation \equiv_{ι} . Or dans le cas où cette relation correspond à l'égalité, c'est-à-dire lorsque les modèles considérés sont des modèles réduits par rapport à \equiv_{ι} , il est possible de simplifier la définition de préordre.

Définition 10 (Préordre sur les modèles réduits) *Etant donné deux modèles $\mathbb{M}_1[\rho_1] = (\mathbb{P}_1[\rho_1], \|\mathcal{R}\|_{\Sigma_1})$ et $\mathbb{M}_2[\rho_2] = (\mathbb{P}_2[\rho_2], \|\mathcal{R}\|_{\Sigma_2})$ respectivement basés sur*

6. Une relation $R \subseteq X \times Y$ est dite fonctionnelle ssi pour tout x dans X et pour tout y et z dans Y si $(x, y) \in R$ et $(x, z) \in R$ alors $y = z$.

7. Une relation $R \subseteq X \times Y$ est injective ssi pour tout x et z dans X et y dans Y , si $(x, y) \in R$ et $(z, y) \in R$ alors $x = z$.

les politiques $\mathbb{P}_1[\rho_1] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_1, \Omega_1)$ et $\mathbb{P}_2[\rho_2] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_2, \Omega_2)$ tels que $\mathbb{M}_1[\rho_1]$ et $\mathbb{M}_2[\rho_2]$ soient des modèles réduits construits à partir de \equiv , $\mathbb{M}_1[\rho_1]$ est plus restrictif que $\mathbb{M}_2[\rho_2]$, ce que nous notons $\mathbb{M}_1[\rho_1] \trianglelefteq \mathbb{M}_2[\rho_2]$, ssi il existe une relation $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ totale à gauche, injective et fonctionnelle telle que :

$$\begin{aligned} & \forall \tau_1 : \mathcal{R} \times \Sigma_1 \rightarrow \mathcal{D} \times \Sigma_1 \quad \forall \Sigma_I^1 \subseteq \Sigma_1 \\ & \mathbb{M}_1[\rho_1] \vdash (\tau_1, \Sigma_I^1) \\ \Rightarrow & \exists \tau_2 : \mathcal{R} \times \Sigma_2 \rightarrow \mathcal{D} \times \Sigma_2 \quad \exists \Sigma_I^2 \subseteq \Sigma_2 \\ & \mathbb{M}_2[\rho_2] \vdash (\tau_2, \Sigma_I^2) \wedge (\tau_1, \Sigma_I^1) \stackrel{\kappa_\Sigma}{\sim} (\tau_2, \Sigma_I^2) \end{aligned}$$

Il est alors possible de montrer qu'un modèle est plus restrictif qu'un autre (selon la définition 9) ssi le modèle réduit du premier est plus restrictif que le modèle réduit du deuxième (selon la définition 10). Pour cela, on montre (Morisset, 2007) tout d'abord que si une implantation I_1 est simulée par une implantation I_2 , alors « l'implantation réduite » de I_1 est simulée par « l'implantation réduite » de I_2 :

$$(\tau_1, \Sigma_I^1) \stackrel{\kappa_\Sigma}{\sim} (\tau_2, \Sigma_I^2) \Rightarrow (\#(\tau_1), \hat{e}_1(\Sigma_I^1)) \stackrel{\kappa_\Sigma^\uparrow}{\sim} (\#(\tau_2), \hat{e}_2(\Sigma_I^2))$$

où $\kappa_\Sigma^\uparrow = \{(e_1(\sigma_1), e_2(\sigma_2)) \mid (\sigma_1, \sigma_2) \in \kappa_\Sigma\}$.

Nous sommes à présent en mesure de démontrer que deux modèles sont ordonnés par \triangleleft ssi leurs modèles réduits respectifs le sont par \trianglelefteq .

Théorème 1 $\mathbb{M}_1[\rho_1] \triangleleft \mathbb{M}_2[\rho_2] \Leftrightarrow \mathbb{M}_1^\#[\rho_1] \trianglelefteq \mathbb{M}_2^\#[\rho_2]$

Ce théorème permet de comparer deux modèles entre eux en considérant leurs modèles réduits. Cette comparaison est *a priori* plus simple, car un modèle réduit possède moins d'implantations que le modèle à partir duquel il a été obtenu par réduction. Quoi qu'il en soit, même en comparant des modèles réduits, le nombre d'implantations à simuler reste relativement important. Nous introduisons dans la section suivante des techniques permettant de réduire, sous certaines conditions, le nombre d'implantations à considérer.

3.3. Propriétés sur les relations de simulation

Pour prouver qu'un modèle est plus restrictif qu'un autre, il est souhaitable de limiter le nombre d'implantations à considérer. En pratique, une solution pour limiter le nombre d'implantations à considérer lors de la comparaison de deux modèles consiste à définir un « plongement » de Σ_1 vers Σ_2 satisfaisant de « bonnes propriétés ». On peut alors définir une relation de simulation κ_Σ à partir de ce plongement. En fonction des propriétés vérifiées par la relation $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$, le théorème 2 permet de comparer deux modèles $\mathbb{M}_1[\rho_1]$ et $\mathbb{M}_2[\rho_2]$ sans avoir à considérer toutes les implantations de $\mathbb{M}_1[\rho_1]$. Les « bonnes propriétés » que la relation κ_Σ doit vérifier sont définies comme suit :

– $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ est \mathcal{W} -monotone ssi :

$$\begin{aligned} & \forall \sigma_1, \sigma'_1 \in \Sigma_1 \quad \forall \sigma_2, \sigma'_2 \in \Sigma_2 \\ & (\mathcal{W}(\sigma_1) \subseteq \mathcal{W}(\sigma'_1) \wedge (\sigma_1, \sigma_2) \in \kappa_\Sigma \wedge (\sigma'_1, \sigma'_2) \in \kappa_\Sigma) \Rightarrow \mathcal{W}(\sigma_2) \subseteq \mathcal{W}(\sigma'_2) \end{aligned}$$

– Etant donné deux politiques $\mathbb{P}_1[\rho_1] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_1, \Omega_1)$ et $\mathbb{P}_2[\rho_2] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_2, \Omega_2)$, $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ est dite Ω -préservante ssi :

$$\forall \sigma_1 \in \Sigma_1 \quad \forall \sigma_2 \in \Sigma_2 \quad ((\sigma_1, \sigma_2) \in \kappa_\Sigma \wedge \Omega_1(\sigma_1)) \Rightarrow \Omega_2(\sigma_2)$$

– Etant donné deux modèles $\mathbb{M}_1[\rho_1] = (\mathbb{P}_1[\rho_1], \|\mathcal{R}\|_{\Sigma_1})$ et $\mathbb{M}_2[\rho_2] = (\mathbb{P}_2[\rho_2], \|\mathcal{R}\|_{\Sigma_2})$, $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ est dite $\|\mathcal{R}\|_\Sigma$ -préservante ssi :

$$\begin{aligned} & \forall \sigma_1 \in \Sigma_1 \quad \forall \sigma_2 \in \Sigma_2 \quad \forall R \in \mathcal{R} \\ & ((\sigma_1, \sigma_2) \in \kappa_\Sigma \wedge (R, \sigma_1) \in \|\mathcal{R}\|_{\Sigma_1}) \Rightarrow (R, \sigma_2) \in \|\mathcal{R}\|_{\Sigma_2} \end{aligned}$$

Le théorème suivant montre que si une relation de simulation κ_Σ entre deux modèles $\mathbb{M}_1[\rho_1]$ et $\mathbb{M}_2[\rho_2]$ est \mathcal{W} -monotone, il est possible de prouver que toute implantation correcte de $\mathbb{M}_1[\rho_1]$ inférieure selon \sqsubseteq à une implantation simulable par une implantation correcte de $\mathbb{M}_2[\rho_2]$ est également simulable. Si la relation κ_Σ est Ω -préservante et $\|\mathcal{R}\|_\Sigma$ -préservante, alors on peut montrer directement que toute implantation correcte de $\mathbb{M}_1[\rho_1]$ est simulable par une implantation correcte de $\mathbb{M}_2[\rho_2]$.

Théorème 2 Soit $\mathbb{M}_1[\rho_1] = (\mathbb{P}_1[\rho_1], \|\mathcal{R}\|_{\Sigma_1})$ et $\mathbb{M}_2[\rho_2] = (\mathbb{P}_2[\rho_2], \|\mathcal{R}\|_{\Sigma_2})$ deux modèles de contrôle d'accès basés respectivement sur les politiques $\mathbb{P}_1[\rho_1] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_1, \Omega_1)$ et $\mathbb{P}_2[\rho_2] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_2, \Omega_2)$, et $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ une relation totale à gauche, injective, fonctionnelle et \mathcal{W} -monotone.

$$\begin{aligned} & 1) \\ & \forall (\tau_1, \Sigma_I^1), (\tau'_1, \Sigma_I'^1), (\tau'_2, \Sigma_I'^2) \\ & \left(\begin{array}{l} \mathbb{M}_1[\rho_1] \vdash (\tau_1, \Sigma_I^1) \wedge \mathbb{M}_1[\rho_1] \vdash (\tau'_1, \Sigma_I'^1) \wedge \mathbb{M}_2[\rho_2] \vdash (\tau'_2, \Sigma_I'^2) \\ \wedge (\tau_1, \Sigma_I^1) \sqsubseteq (\tau'_1, \Sigma_I'^1) \wedge (\tau'_1, \Sigma_I'^1) \stackrel{\kappa_\Sigma}{\sim} (\tau'_2, \Sigma_I'^2) \end{array} \right) \\ & \Rightarrow \exists (\tau_2, \Sigma_I^2) \quad \mathbb{M}_2[\rho_2] \vdash (\tau_2, \Sigma_I^2) \wedge (\tau_1, \Sigma_I^1) \stackrel{\kappa_\Sigma}{\sim} (\tau_2, \Sigma_I^2) \end{aligned}$$

2) Si κ_Σ est Ω -préservante et $\|\mathcal{R}\|_\Sigma$ -préservante, alors pour toute implantation correcte (τ_1, Σ_I^1) , il existe une implantation correcte (τ_2, Σ_I^2) telle que $(\tau_1, \Sigma_I^1) \stackrel{\kappa_\Sigma}{\sim} (\tau_2, \Sigma_I^2)$

Ce théorème permet de montrer que si une implantation correcte d'un modèle est simulable, alors toute implantation qui lui est inférieure est aussi simulable. Il permet également de montrer que si la relation de simulation respecte des « bonnes propriétés », alors toute implantation du modèle est simulable. Nous pouvons à présent montrer que si pour toute implantation d'un modèle $\mathbb{M}_1[\rho_1]$, il existe une implantation qui lui est supérieure par \sqsubseteq et qui est simulable par une implantation de $\mathbb{M}_2[\rho_2]$, alors $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$. Nous montrons également que si la relation de simulation vérifie de « bonnes propriétés », on obtient directement $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$.

Théorème 3 *Etant donné deux modèles de contrôle d'accès $\mathbb{M}_1[\rho_1] = (\mathbb{P}_1[\rho_1], \|\mathcal{R}\|_{\Sigma_1})$ et $\mathbb{M}_2[\rho_2] = (\mathbb{P}_2[\rho_2], \|\mathcal{R}\|_{\Sigma_2})$ basés respectivement sur les politiques $\mathbb{P}_1[\rho_1] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_1, \Omega_1)$ et $\mathbb{P}_2[\rho_2] = (\mathcal{S}, \mathcal{O}, \mathcal{A}, \Sigma_2, \Omega_2)$, et $\kappa_\Sigma \subseteq \Sigma_1 \times \Sigma_2$ une relation totale à gauche, \mathcal{W} -monotone, ι -fonctionnelle et ι -injective.*

1) *Si pour toute implantation $(\tau_1, \Sigma_I^1) \equiv_{\iota_1}$ -préservante telle que $\mathbb{M}_1[\rho_1] \vdash (\tau_1, \Sigma_I^1)$, il existe une implantation $(\tau'_1, \Sigma_I'^1) \equiv_{\iota_1}$ -préservante telle que $\mathbb{M}_1[\rho_1] \vdash (\tau'_1, \Sigma_I'^1)$ et $(\tau_1, \Sigma_I^1) \sqsubseteq (\tau'_1, \Sigma_I'^1)$ et s'il existe une implantation $(\tau'_2, \Sigma_I'^2) \equiv_{\iota_2}$ -préservante telle que $\mathbb{M}_2[\rho_2] \vdash (\tau'_2, \Sigma_I'^2)$ vérifiant $(\tau'_1, \Sigma_I'^1) \stackrel{\kappa_\Sigma}{\sim} (\tau'_2, \Sigma_I'^2)$, alors $\mathbb{M}_1[\rho_1] \triangleleft \mathbb{M}_2[\rho_2]$.*

2) *Si κ_Σ est Ω -préservante et $\|\mathcal{R}\|_\Sigma$ -préservante, alors $\mathbb{M}_1[\rho_1] \triangleleft \mathbb{M}_2[\rho_2]$.*

Ainsi, avec le théorème 3, pour montrer qu'un modèle est plus restrictif qu'un autre, il suffit de montrer que toutes les implantations \sqsubseteq -maximales⁸ sont simulables. Ceci n'est cependant vrai que dans le cas où toute implantation est inférieure à une implantation maximale. Dans le cas où il existe une chaîne infinie croissante d'implantations, le point 1) de ce théorème n'est pas applicable. Néanmoins, dans la plupart des modèles, l'ensemble des états est fini, ce qui implique que le nombre d'implantations possibles est fini, et il n'existe alors pas de chaîne infinie croissante. Notons également que si le point 2) du théorème 3 semble *a priori* plus simple à appliquer, il n'est cependant pas tout le temps possible de construire une relation κ_Σ respectant à la fois la politique de sécurité et la sémantique faible des requêtes, bien qu'il soit néanmoins possible de montrer que toute implantation correcte est simulable par une implantation correcte.

4. Applications

Nous illustrons ici rapidement l'utilisation des concepts introduits plus haut pour comparer des modèles classiques de contrôle d'accès.

4.1. Spécifications, implantations et codage de modèles classiques

L'ensemble des définitions et résultats présentés dans cet article ont été utilisés pour définir et comparer des politiques classiques de contrôle d'accès. Les modèles suivants ont été définis et des implantations de ces modèles ont été prouvées correctes.

– Modèle ACL – *Access Control List* – (Brecht *et al.*, 2007)

$$\mathbb{M}_{ACL}[\rho_{ACL}] \vdash (\tau_{ACL}, \Sigma_I^{ACL})$$

– Modèle de Bell et LaPadula – (Morisset, 2007)

$$\mathbb{M}_{BLP}[\rho_{BLP}] \vdash (\tau_{BLP}, \Sigma_I^{BLP})$$

8. Une implantation (τ, Σ_I) d'un modèle $\mathbb{M}[\rho]$ est \sqsubseteq -maximale ssi il n'existe pas une autre implantation (τ', Σ_I') de $\mathbb{M}[\rho]$ telle que $(\tau, \Sigma_I) \sqsubset (\tau', \Sigma_I')$.

– Modèle de la Muraille de Chine – (Morisset, 2007)

$$\mathbb{M}_{CW}[\rho_{CW}] \vdash (\tau_{CW}, \Sigma_I^{CW})$$

– Modèle RBAC – *Role Based Access Control* – (Habib, 2007)

$$\mathbb{M}_{RBAC}[\rho_{RBAC}] \vdash (\tau_{RBAC}, \Sigma_I^{RBAC})$$

Ces développements ont été validés par une implantation du cadre sémantique d'une part, et d'autre part des modèles étudiés qui ont été implantés à partir du cadre. Ces implantations ont été obtenues à l'aide de l'atelier Focal (Rioboo *et al.*, 2003), qui fournit un environnement de développement reposant sur un langage fonctionnel muni de traits objets permettant d'écrire au sein d'un même programme des fonctions, des propriétés et des preuves. Notre objectif est d'avoir à terme une librairie certifiée de modèles de contrôle d'accès. Pour réutiliser un modèle déjà défini, l'utilisateur n'aura qu'à définir les éléments spécifiques de son système (tels que les sujets, les objets ou encore le paramètre de sécurité). Les traits objets de Focal lui permettront alors d'hériter des preuves de correction (qui ne dépendent pas de ces éléments spécifiques).

4.2. Comparaison de modèles : méthodologie

La démarche que nous avons adoptée pour établir que $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$ se décompose en deux étapes principales. Dans un premier temps, on construit un modèle intermédiaire $\mathbb{M}_{12}[\rho_2]$ correspondant au modèle $\mathbb{M}_1[\rho_1]$ exprimé dans le formalisme de $\mathbb{M}_2[\rho_2]$. Pour ce faire, il faut bien sûr commencer par interpréter le paramètre de sécurité ρ_1 par un paramètre de sécurité $\rho_2 = \kappa_\rho(\rho_1)$, puis considérer les états. Cette interprétation permet de définir un prédicat de sécurité Ω_{12} sur Σ_2 à partir duquel le modèle $\mathbb{M}_{12}[\kappa_\rho(\rho_1)]$ est défini. Ce mécanisme de traduction permet de définir une relation de simulation à partir de laquelle on établit $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_{12}[\kappa_\rho(\rho_1)]$. Il faut ensuite montrer que la politique définie par le prédicat Ω_{12} est plus restrictive que celle définie par Ω_2 , c'est-à-dire :

$$\forall \sigma \in \Sigma_2 \quad \Omega_{12}(\sigma) \Rightarrow \Omega_2(\sigma)$$

Dans ce cas, on montre facilement (Morisset, 2007) que $\mathbb{M}_{12}[\kappa_\rho(\rho_1)] \prec \mathbb{M}_2[\rho_2]$. Finalement, on a montré :

$$\forall \rho_1 \exists \rho_2 \quad \mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$$

En effet, il suffit alors de poser $\rho_2 = \kappa_\rho(\rho_1)$.

La méthodologie esquissée ci-avant a été utilisée avec succès (Morisset, 2007; Habib, 2007) pour comparer entre eux les modèles de la Muraille de Chine, de Bell et LaPadula et RBAC96 (à base de rôles). Nous présentons ici les grandes lignes du raisonnement permettant de montrer que le modèle $\mathbb{M}_{CW}[\rho_{CW}]$ de la Muraille de Chine est strictement plus restrictif que le modèle $\mathbb{M}_{BLP}[\rho_{BLP}]$ de Bell et LaPadula.

Traduction : construction d'un modèle intermédiaire. Pour montrer que le modèle de la Muraille de Chine est plus restrictif que le modèle de Bell et LaPadula,

il faut tout d'abord donner une interprétation des concepts de $\mathbb{M}_{CW}[\rho_{CW}]$ par des concepts de $\mathbb{M}_{BLP}[\rho_{BLP}]$. Il s'agit d'exprimer à l'aide d'un treillis de niveaux de sécurité ρ_{LCW} les notions de compagnies et de classes de conflits présentes dans le paramètre ρ_{CW} de la Muraille de Chine. Ce treillis a bien sûr une forme particulière puisqu'il est issu d'une fonction de traduction κ_ρ qui permet d'obtenir un treillis $\kappa_\rho(\rho_{CW}) = \rho_{LCW}$ à partir du paramètre ρ_{CW} . On cherche donc à montrer que $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$. Il s'agit alors de spécifier comment représenter un état du système décrit dans le formalisme de la Muraille de Chine par un état équivalent décrit dans le formalisme de Bell et LaPadula. Concrètement, on définit donc une relation $\kappa_\Sigma \subseteq \Sigma_{CW} \times \Sigma_{BLP}$ qui permet de relier les états des deux formalismes et qui sera utilisée comme relation de simulation par la suite. Il reste alors à reformuler le prédicat Ω_{CW} qui spécifie la politique de la Muraille de Chine par un prédicat Ω_{LCW} exprimé dans le formalisme de Bell et LaPadula. On obtient finalement un nouveau modèle $\mathbb{M}_{LCW}[\rho_{LCW}]$. C'est à partir de ce modèle intermédiaire que nous allons pouvoir montrer que $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$. Nous procédons en deux étapes : nous montrons tout d'abord $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{LCW}[\rho_{LCW}]$ puis nous montrons $\mathbb{M}_{LCW}[\rho_{LCW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$.

Comparaison du modèle original avec le modèle intermédiaire. Nous avons montré que $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{LCW}[\rho_{LCW}]$ en utilisant le théorème 3. Nous avons donc tout d'abord montré que la relation κ_Σ définie à l'étape précédente était totale à gauche, \mathcal{W} -monotone, ι -fonctionnelle et ι -injective. Nous avons ensuite prouvé le résultat de deux manières différentes.

1) Nous avons prouvé que toute implantation correcte de la Muraille de Chine est inférieure (selon \sqsubseteq) à l'implantation classique $(\tau_{CW}, \Sigma_I^{CW})$ de ce modèle (*i.e.* $(\tau_{CW}, \Sigma_I^{CW})$ est la seule implantation maximale de la Muraille de Chine), et qu'il existe une implantation $(\tau_{LCW}, \Sigma_I^{LCW})$ correcte du modèle de Bell et LaPadula qui simule $(\tau_{CW}, \Sigma_I^{CW})$. Le point 1) du théorème 3 nous permet alors de conclure que $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{LCW}[\rho_{LCW}]$.

2) Nous avons prouvé que la relation κ_Σ est Ω -préservante et $\llbracket \mathcal{R} \rrbracket_\Sigma$ -préservante. Le point 2) du théorème 3 nous permet alors de conclure que $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{LCW}[\rho_{LCW}]$.

Comparaison du modèle intermédiaire avec le modèle « cible ». Une fois la politique de la Muraille de Chine exprimée par le prédicat Ω_{LCW} dans le formalisme du modèle de Bell et LaPadula, il est facile de montrer que tout état vérifiant le prédicat Ω_{LCW} vérifie aussi le prédicat définissant la politique de Bell et LaPadula et on montre alors facilement que $\mathbb{M}_{LCW}[\rho_{LCW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$ ce qui, par transitivité, nous permet finalement d'établir que $\mathbb{M}_{CW}[\rho_{CW}] \triangleleft \mathbb{M}_{BLP}[\rho_{LCW}]$.

Cette méthodologie repose sur l'idée de séparer de manière claire les étapes de traduction et de comparaison. En revanche, pour montrer qu'un modèle $\mathbb{M}_1[\rho_1]$ n'est pas plus restrictif qu'un modèle $\mathbb{M}_2[\rho_2]$, on procède de manière différente. En effet, pour ce faire, on montre que :

$$\exists \rho_1 \forall \rho_2 \quad \mathbb{M}_1[\rho_1] \not\triangleleft \mathbb{M}_2[\rho_2]$$

Il suffit donc de concevoir une valeur pour ρ_1 qui ne puisse pas être associée à un paramètre ρ_2 tel que $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$. On montre en fait par un argument de cardinalité sur les ensembles d'états qu'il n'existe pas de relation de simulation permettant d'établir $\mathbb{M}_1[\rho_1] \prec \mathbb{M}_2[\rho_2]$. Cette étape est grandement facilitée si l'on considère les modèles réduits (le théorème 1 garantit la validité de ce procédé). Ainsi, pour montrer que $\mathbb{M}_{BLP}[\rho_{BLP}] \not\prec \mathbb{M}_{CW}[\rho_{CW}]$, nous nous sommes appuyés sur le fait que dans le modèle de la Muraille Chine, il n'était pas possible d'interdire un accès en lecture si aucun autre accès n'est présent, contrairement au modèle de Bell et La Padula. Ainsi, pour la Muraille de Chine, le cardinal de l'ensemble des classes d'équivalence selon $\equiv_{\mathcal{W}}$ est inférieur au cardinal de l'ensemble des classes d'équivalence selon $\equiv_{\mathcal{W}}$ pour le modèle de Bell et LaPadula, ce qui permet de montrer facilement qu'il n'existe pas de relation de simulation ι -injective.

En suivant cette méthodologie, nous avons également montré que :

$$\begin{aligned} \mathbb{M}_{BLP}[\rho_{BLP}] \prec \mathbb{M}_{RBLP}[\rho_{RBLP}] \prec \mathbb{M}_{RBAC}[\rho_{RBAC}] \\ \mathbb{M}_{RBAC}[\rho_{RBAC}] \not\prec \mathbb{M}_{BLP}[\rho_{BLP}] \end{aligned}$$

où $\mathbb{M}_{RBLP}[\rho_{RBLP}]$ représente l'interprétation à base de rôles du modèle de Bell et LaPadula. Il est alors possible de déduire que $\mathbb{M}_{CW}[\rho_{CW}] \prec \mathbb{M}_{RBAC}[\rho_{RBAC}]$. Ces preuves sont détaillées dans (Morisset, 2007; Habib, 2007).

5. Conclusion et perspectives

La sécurité, et plus particulièrement le contrôle d'accès, sont des problématiques actuelles en informatique. En effet, il devient aujourd'hui important de pouvoir contrôler les flots d'informations dans les réseaux et dans les systèmes d'information. Il convient de développer au sein des systèmes informatiques des mécanismes permettant de filtrer les accès afin de ne laisser passer que ceux autorisés. Il s'agit pour cela de définir une politique de sécurité, c'est-à-dire la caractérisation des accès permis. Le programme chargé de mettre en application cette politique, le moniteur de référence, est souvent considéré comme l'une des clés de voûte de la sécurité d'un système. Sa conception et son développement doivent être menés de manière à garantir sa fiabilité et sa sûreté. En effet, toute faille au sein de ce programme pourrait entraîner des violations de la politique de sécurité. L'emploi des méthodes formelles dans le développement d'un moniteur de référence permet de garantir que certaines propriétés sont toujours respectées.

Dans cet article nous avons introduit un cadre formel permettant de définir *a priori* n'importe quel modèle de contrôle d'accès, et fournissant les outils nécessaires pour comparer deux modèles entre eux. Il est en effet souhaitable de disposer d'un cadre uniforme dans lequel puissent s'exprimer les modèles de contrôle d'accès que nous envisageons : il s'agit à la fois d'identifier les « ingrédients » communs aux politiques de contrôle d'accès, d'exprimer les propriétés génériques qu'ils vérifient, d'en prouver certaines et de formaliser les politiques envisagées comme des instances du cadre générique. Ce cadre différencie la notion de politique de contrôle d'accès de celle de mo-

dèle de contrôle d'accès. Une politique est la spécification du « quoi », dans le sens où elle définit quelles sont les entités et quels sont les états (sûrs et non sûrs). Un modèle est la spécification du « comment », dans le sens où il décrit comment passer d'un état à un autre. Une relation de préordre a été définie sur les implantations d'un modèle. Cette relation correspond à une notion de restriction : intuitivement, l'implantation la plus petite d'un modèle est celle qui permet de faire le moins de choses. Conjointement à la notion de modèle, nous avons introduit la notion de modèle réduit, qui s'obtient en ignorant l'information « inutile », c'est-à-dire l'information non discriminante au regard de la politique de sécurité. Nous avons également proposé un préordre sur les modèles permettant de comparer formellement deux modèles de contrôle d'accès. Ce préordre exprime une notion intuitive de « plongement » : un modèle est plus restrictif qu'un autre si toute implantation du premier est simulable par une implantation du deuxième. La relation de préordre sur les implantations ainsi que la notion de modèle réduit nous ont permis de montrer que dans certains cas, pour prouver qu'un modèle est plus restrictif qu'un autre, il suffit de savoir simuler toute implantation maximale du premier par une implantation du deuxième. De plus, si la relation de simulation préserve la politique de sécurité ainsi que la sémantique des requêtes, alors il est possible de montrer directement, sans considérer les implantations, qu'un modèle est plus restrictif qu'un autre. Cette dernière approche semble *a priori* plus simple, mais il est en fait difficile de construire une relation de simulation *ex nihilo* qui préserve à la fois la politique de sécurité et la sémantique des requêtes. Cette construction possède en effet un aspect opérationnel important (on relie des états « pouvant faire les mêmes choses »), et il est souvent plus simple de définir la relation de simulation à partir des deux implantations que l'on cherche à simuler, puis de prouver que cette relation vérifie les bonnes propriétés. Nous avons ensuite instancié ce cadre formel pour obtenir trois modèles de contrôle d'accès parmi les plus connus : le modèle de Bell de LaPadula, celui de la Muraille de Chine et le modèle à base de rôles RBAC96. Enfin, nous avons pu montrer, en utilisant le cadre sémantique défini dans cet article, que le modèle de la Muraille de Chine est plus strictement plus restrictif que celui de Bell et LaPadula qui est lui-même strictement plus petit que RBAC96. C'est à notre connaissance la première fois que ce résultat est démontré de manière formelle.

L'ensemble des travaux décrits ci-avant méritent à présent d'être poursuivis. Tout d'abord, l'indispensable travail de formalisation a mis en relief certaines confusions : plusieurs définitions non équivalentes d'une même propriété coexistent dans la littérature. Nous envisageons d'étoffer la bibliothèque de modèles formels de contrôle d'accès en considérant des modèles discrétionnaires (mécanismes de listes, de délégation, de tickets, de groupes d'utilisateurs...) largement utilisés dans les systèmes à la UNIX. A partir de ces formalisations, il sera alors possible de classer l'ensemble des modèles les plus utilisés dans les systèmes actuels. Cette classification repose sur la notion de comparaison de modèles définie dans le cadre sémantique défini. Elle permettra d'identifier les modèles dont les implantations peuvent être simulées par des implantations de modèles offrant un pouvoir d'expression plus riche, mais elle permettra aussi d'identifier de manière précise les limites de ces modèles. Un tel développement permet de fournir des critères pour le choix d'un modèle de sécurité dans

un système d'information et permet également de fournir des outils de réutilisation d'implantations de modèles.

Nous souhaitons aussi « comparer » les « comparaisons de modèles de contrôle d'accès ». En effet, quelques travaux ont déjà eu lieu sur ce sujet mais ils sont encore parcellaires : (Tripunitara *et al.*, 2004) envisagent la comparaison de politiques de contrôle d'accès en termes de puissance d'expression, (Chander *et al.*, 2001) utilise des techniques de simulation pour comparer des modèles de contrôle d'accès discrétionnaire, (Tschantz *et al.*, 2006) envisagent la comparaison de politiques sous l'angle de la combinaison de politiques. Chacune de ces approches adoptant un point de vue différent sur la notion de contrôle d'accès, il est donc difficile de les comparer directement. Notons toutefois que la plupart de ces approches abordent principalement la comparaison de modèles discrétionnaires et ne distinguent pas la sémantique des requêtes des fonctions de transition qui permettent d'appliquer ces requêtes comme nous le faisons. Elles sous-entendent donc que les politiques sont mises en œuvre de la manière la moins restrictive possible (au sens de la relation \sqsubseteq introduite dans cet article). En revanche, ces approches envisagent les requêtes administratives (dont l'effet est de modifier les fonctions de sécurité d'un état). Pour prendre en compte ce type de requêtes, il nous faut pouvoir considérer des relations de simulation « faibles ». En effet, une transition effectuée à partir d'une requête administrative d'un modèle peut nécessiter l'application de plusieurs requêtes administratives d'un autre modèle pour produire les mêmes effets (il se pose alors le problème du maintien de la politique sur les états intermédiaires). Nous étudions actuellement ces aspects. Quoi qu'il en soit, toutes ces approches portent sur le même objet et méritent d'être reconsidérées et étendues dans un cadre uniforme afin d'en étudier les liens et d'en dégager de nouvelles techniques de réutilisation. Cette étude permettrait donc d'outiller (ou d'enrichir) le cadre sémantique proposé pour prendre en compte ces approches.

Enfin, l'étude de la comparaison de modèles de contrôle d'accès est un premier pas vers l'étude de la composition de ces modèles. Cette problématique mérite aussi d'être développée puisqu'elle correspond à un problème actuel concret dans les systèmes d'information. En effet, dans la pratique, un sujet accède généralement à un objet en passant au travers de plusieurs filtres (par exemple un employé accède aux données du système d'information de son entreprise régi par une certaine politique, après avoir pénétré dans les locaux de cette entreprise, eux-mêmes régis par une autre politique de contrôle d'accès). Il existe évidemment plusieurs procédés pour composer des politiques de sécurité. Nous souhaitons étudier cette problématique afin de formaliser les concepts liés à la composition pour pouvoir exprimer les propriétés de sécurité que les mécanismes de composition envisagés peuvent garantir.

Remerciements

Nous remercions vivement Thérèse Hardin pour toutes les discussions fructueuses que nous avons eues à propos de ce travail ainsi que les rapporteurs anonymes de cet article pour leurs remarques constructives.

6. Bibliographie

- Amey P., « Dear Sir, Yours Faithfully : an Everyday Story of Formality », *Practical Elements of Safety, Proceedings of the Twelfth Safety-critical Systems Symposium*, Springer-Verlag, p. 3-15, 2004.
- Anderson J. P., Computer Security Technology Planning Study, Technical Report n° ESD-TR-73-51, USAF Electronic Systems Division, Hanscom Air Force Base, Bedford, Massachusetts, October, 1972.
- Bell D., LaPadula L., Secure Computer Systems : a Mathematical Model, Technical Report n° MTR-2547 (Vol. II), MITRE Corp., Bedford, MA, May, 1973.
- Blond J., Morisset C., « Formalisation et implantation d'une politique de sécurité d'une base de données », in INRIA (ed.), *17ème Journées Francophones des Langages Applicatifs, JFLA'2006*, p. 71-86, 2006.
- Blond J., Morisset C., « Un moniteur de référence sûr d'une base de données », *Technique et Science Informatiques*, vol. 26, n° 9, p. 1091-1110, 2007.
- Brecht F., Kadja A.-D., « Implantation d'une politique de contrôle d'accès discétionnaire avec Focal », Master's thesis, Université Pierre & Marie Curie, Paris, France, 2007.
- Brewer D. F. C., Nash M. J., « The Chinese Wall Security Policy », *Proceedings of the IEEE Symposium on Security and Privacy*, p. 329-339, May, 1989.
- CC, *Common Criteria for Information Technology Security Evaluation, v3.1.* 2006, <http://www.commoncriteriaportal.org/>.
- Chander A., Mitchell J., Dean D., « A State-Transition Model of Trust Management and Access Control », *Proceedings of the 14th IEEE Computer Security Foundations Workshop CSFW*, IEEE Computer Society Press, p. 27-43, 2001.
- Cohen E., Thomas R. K., Winsborough W., Shands D., « Models for coalition-based access control (CBAC) », *SACMAT '02 : Proceedings of the seventh ACM symposium on Access control models and technologies*, ACM Press, p. 97-106, 2002.
- Ferraiolo D. F., Kuhn D. R., « Role-Based Access Control », *Proceedings of the 15th National Computer Security Conference*, 1992.
- Habib L., « Formalisation, comparaison et implantation d'un modèle de contrôle d'accès à base de rôles », Master's thesis, Université Pierre & Marie Curie, Paris, France, 2007.
- Harrison M. A., Ruzzo W. L., Ullman J. D., « Protection in operating systems », *Commun. ACM*, vol. 19, n° 8, p. 461-471, 1976.
- Jaume M., Morisset C., « Formalisation and implementation of Access control models », *Information Assurance and Security (IAS'05) International Conference on Information Technology, ITCC*, IEEE CS Press, p. 703-708, 2005.
- Jaume M., Morisset C., « A formal approach to implement access control », *Journal of Information Assurance and Security*, vol. 2, p. 137-148, June, 2006a.
- Jaume M., Morisset C., « Towards a formal specification of access control », in P. Degano, R. Kusters, L. Vigano, S. Zdancewic (eds), *Proceedings of the Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis, FCS-ARSPA'06*, p. 213-232, 2006b.
- Jaume M., Morisset C., « Contrôler le contrôle d'accès », *AFADL'06, Approches Formelles dans l'Assistance au Développement de Logiciels*, Namur, Belgique, juin, 2007.

- Kalam A. A. E., Baida R. E., Balbiani P., Benferhat S., Cuppens F., Deswarte Y., Miège A., Saurel C., Trouessin G., « Organization Based Access Control », *Policy'2003*, Como, Italie, June, 2003.
- Levy H., *Capability-Based Computer Systems*, Digital Press, Bedford, MA, 1984.
- Morisset C., Formalisation et Implantation d'un modèle de contrôle d'accès dans l'atelier Focal, Rapport de DEA, Université Paris 6, 2004.
- Morisset C., Sémantique des systèmes de contrôle d'accès, PhD thesis, Université Pierre et Marie Curie - Paris 6, 2007.
- Rioboo R., Doligez D., Prevosto V., Jaume M., Maarek M., Dubois C., Fechter S., Ménissier-Morain V., Pons O., Delahaye D., Viguié V., Hardin T., *FoC, version 0.4 Tutorial and reference manual*, LIP6 – INRIA – CNAM. jui, 2003, Distribution available at : <http://focal.inria.fr>.
- Thomas R. K., « Team-based access control (TMAC) : a primitive for applying role-based access controls in collaborative environments », *RBAC '97 : Proceedings of the second ACM workshop on Role-based access control*, ACM Press, p. 13-19, 1997.
- Tripunitara M., Li N., « Comparing the Expressive Power of Access Control Models », *SIG-SAC : 11th ACM Conference on Computer and Communications Security*, ACM SIGSAC, 2004.
- Tschantz M., Krishnamurthi S., « Towards reasonability properties for access-control policy languages », in D. Ferraiolo, I. Ray (eds), *SACMAT 2006, 11th ACM Symposium on Access Control Models and Technologies, Proceedings*, ACM, p. 160-169, 2006.

Article reçu le 19 octobre 2007

Accepté après révisions le 22 mai 2008

Mathieu Jaume est maître de conférences au LIP6. Ses activités de recherche portent sur les spécifications/preuves formelles, les modèles de contrôle d'accès et la sémantique des langages.

Charles Morisset a récemment soutenu sa thèse de doctorat à l'université Pierre et Marie Curie sur la sémantique des systèmes de contrôle d'accès et est actuellement en Postdoc à l'International Institute for Software Technology, centre de recherche de l'université des Nations-Unies, à Macao. Ses travaux portent sur les méthodes formelles en général et plus particulièrement sur la spécification et la formalisation de modèles de contrôle d'accès.