# *Sécurité des systèmes d'information et de communication dans le domaine de la santé*

Anas Abou El Kalam ; Yves Deswarte
*LAAS-CNRS — 7 avenue du Colonel Roche — 31077 Toulouse Cedex 4 — France*
*{anas, Yves.Deswarte}@laas.fr*

**Résumé** : Alors que l'informatisation s'impose dans des domaines complexes, coopératifs et largement distribués comme le commerce électronique et la télémédecine, il devient de plus en plus nécessaire d'avoir une confiance élevée dans les traitements, la stratégie et la distribution des données informatiques. Cet article propose une démarche de sécurisation des systèmes d'informations et de communication de santé. La méthode présentée réalise un bon compromis entre le respect du principe du moindre privilège et la flexibilité du contrôle d'accès, de façon à ne pas gêner le travail des personnels soignants, tout en respectant les droits des patients. La première étape consiste à décrire le système, identifier les informations à protéger et caractériser les menaces. La politique de sécurité vient ensuite décrire comment contrer ces menaces, en exprimant les besoins de sécurité et les règles qui expliquent comment l'information sensible et les autres ressources sont gérées protégées et distribuées dans le système. La politique de sécurité que nous présentons a l'originalité de tenir compte du contexte, de l'interopérabilité et d'être suffisamment souple pour prendre en compte toute amélioration, changement ou mise à jour des éléments en relation avec la sécurité (objectifs de sécurité, liste des utilisateurs, etc.). Nous représentons cette politique dans un langage formel et nous montrons comment utiliser ce langage pour la vérifier. Nous donnons également diverses indications sur la manière dont cette politique de sécurité peut être mise en œuvre.

**Mots-clés :** Politiques de sécurité, modèles de sécurité, logique déontique, Systèmes d'Information et de communication en santé, mécanismes de sécurité.

## 1 Introduction

La sécurité des systèmes d'information et de communication en santé (SICS) est un problème complexe aux dimensions légales, éthiques, sociales, organisationnelles et techniques. Pour atteindre un niveau de sécurité satisfaisant, une étape primordiale consiste à spécifier simultanément les propriétés désirées et d'établir un cadre réglementaire pour assurer la protection [1]. La notion de politique de sécurité peut se développer selon trois directions distinctes : physique, administrative et logique. La première précise tout ce qui touche à la situation physique du système à protéger. En particulier, y sont définis les éléments critiques et les mesures prises vis-à-vis du vol, des catastrophes, etc. La deuxième décrit les procédures qui touchent à la sécurité d'un point de vue organisationnel (répartition des tâches, séparation des pouvoirs, etc.). La troisième décrit les contrôles d'accès logiques en spécifiant qui a accès à quoi, et dans quelles circonstances. Elle s'intéresse aux phases d'identification, d'authentification et d'autorisation. Ce papier présente une démarche globale de spécification d'une politique d'autorisation fine et flexible, à sa formalisation par un modèle de sécurité, et aux différents mécanismes de sécurité qui permettent de la mettre en oeuvre.

## 2 Définition du problème

Un SICS peut être défini comme un grand réseau dédié à la santé. Il relie des utilisateurs multiples : professionnels de santé, patients, organismes sociaux, etc. Il met en jeu des technologies complexes : communication, traitement, télémédecine, paiement, archivage, et manipule des informations hétérogènes : médicales, paramédicales, médico-administratives et médico-financières. Indispensable pour gérer la complexité et maîtriser les dépenses, le système informatique ne doit pas engendrer de dégradation de la sécurité, que cette dégradation soit due à l'architecture, à l'interaction avec les utilisateurs ou qu'elle résulte d'une attaque malveillante. Au contraire, il doit être possible d'empêcher l'exécution de toute opération non autorisée et de protéger les informations sensibles.

## 2.1 Informations sensibles

L'une des raisons qui nous ont poussé à étudier la sécurité des SICS est la complexité et la sensibilité des toutes les informations y figurant. En effet, les obligations éthiques imposent une protection particulière des données nominatives des patients. On entend par donnée nominative toute donnée décrivant une personne parfaitement identifiée. Malheureusement, il est souvent possible d'identifier un individu par un simple rapprochement de données médicales et/ou sociales et/ou professionnelles. Par exemple, l'âge, le sexe, l'identifiant d'un établissement hospitalier, et les mois de sortie du patient de cet établissement, permettent de l'isoler dans une population. Par conséquent, les données à caractère personnel sont très diverses et même l'utilisation des pseudonymes demeure souvent insuffisante. Les données non nominatives sont également sensibles dans la mesure où leur altération peut induire des erreurs de traitement des données nominatives, des erreurs de diagnostic, de traitement médicaux, de calculs de remboursement, etc. [3].

Diverses lois dressent une liste de ressources et services à protéger. L'Assemblée générale des Nations Unies a adopté, dans sa résolution 45/95 [4], des directives pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Le Conseil de l'Europe a établi des recommandations concernant les banques de données médicales automatisées [5] et les échanges des données de santé dans les hôpitaux [6]. La Commission Européenne a développé la directive [7] relative à la protection des données personnelles et à la libre circulation de ces données. Dans la législation française, la récente loi du 4 mars 2002 [8] définit les droits des malades et décrit les qualités exigées dans le système de santé, le décret 2002-637 [9] restreint les accès aux informations personnelles détenues par les professionnels de santé.

## 2.2 Risques identifiés

L'analyse des risques permet la mise en œuvre d'une politique de sécurité en identifiant les vulnérabilités résiduelles et en évaluant leurs impacts sur la sécurité du système. Avant d'entamer une partie de cette procédure, rappelons tout d'abord quelques définitions [10, 11] :

- Une attaque est une action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité.
- Une intrusion est une faute opérationnelle externe intentionnellement nuisible ayant exploité avec succès une vulnérabilité dans le système.
- Une menace est une violation potentielle d'une propriété de sécurité.
- Une vulnérabilité est une faute accidentelle ou intentionnelle (avec ou sans volonté de nuire), introduite dans la spécification, la conception, la configuration ou dans l'opération du système.

Les couples (menace, vulnérabilité) permettent d'identifier les risques auxquels peuvent être soumis les SICS. Cet article identifie quelques-uns :

- Attribution des données d'un patient à une autre personne (homonymes) ;
- Utilisation illicite des moyens de communication de données ;
- Utilisation (modification, consultation, etc.) non autorisé des données et des programmes ou mauvaise utilisation de ces programmes/données (ex : introduction de virus) ;
- Défaillances survenant lors des mises à jour ; destruction illégitime de données, etc.

Les directives européennes [12] spécifient que le fournisseur d'un service web (ex : datawarehouse) doit prendre les mesures techniques (ex : sauvegardes) et organisationnelles (ex : politique de sécurité) pour garantir la sécurité de ses services. La résolution [4] met en garde contre les pertes accidentelles des informations, les accès non autorisés, les utilisations illégitimes, les virus, etc. La commission d'audit britannique et le « US Government's Office of Technology Assessment » ont confirmé que le domaine de la santé est l'une des cibles les plus attaquées par les utilisateurs malveillants aussi bien internes qu'externes (atteinte à la vie privée, fraudes, perte de données et de logiciels) [13, 14]. En France, le décret [11] identifie des menaces relatives aux accès illégitimes et aux pertes de données, le code de déontologie médicale [15] et le code de santé publique [16] sensibilise les professionnels de santé aux risques liés au secret professionnel. Des statistiques faites aux Etats-Unis [17] ont montré que, dans plus de 30 % des cas, les fichiers médicaux sont indisponibles, et même quand ils sont disponibles, les délais nécessaires pour extraire les informations sont souvent décourageants. Ces taux

élevés ont été argumentés par différentes raisons : patients vus dans plusieurs cliniques le même jour, fichiers gardés par les médecins, suppressions illégitimes des fichiers.

Les intrusions dans les SICS revêtent une importance primordiale. Si les propriétés de sécurité sont violées : le médecin peut prendre des décisions causant des dégâts pour le patient ou pire le tuant, la valeur de l'information comme base de diagnostic est amoindrie et un professionnel de santé appelé à justifier ses actions, pourrait être dans l'incapacité d'utiliser les dossiers informatiques comme preuve.

### *2.3 Besoins de sécurité*

Les risques identifiés dans la section précédente justifient directement un besoin fort en confidentialité, intégrité et disponibilité.

*La confidentialité* est étroitement liée au respect du secret professionnel et de la vie privée des patients. Le médecin doit faire en sorte, lorsqu'il utilise son expérience à des fins de publications scientifiques ou d'enseignement, que l'identification des patients ne soit pas possible ; un utilisateur habilité à comptabiliser les traitements des médecins ou à faire des statistiques ne devrait pas avoir le droit d'accéder aux données nominatives, etc.

*L'intégrité* est la non-occurrence d'altérations inappropriées de l'information. Elle implique que les données et les applications sont valides et qu'elles ne peuvent être changées que par une action autorisée. Elle peut donc être mise en cause par des manipulations erronées mais également par la perte de données accidentelle ou délictueuse. Le problème est d'autant plus complexe que le système est largement distribué et en même temps doit garantir l'exactitude et la cohérence des données même en cas de défaillance. L'intégrité touche également à la validité des données saisies, en particulier, éviter les collisions (obtenir, à partir de données nominatives différentes, un même identifiant anonyme) et les doublons (deux numéros d'hospitalisation identiques pointant sur des variables identifiantes différentes) lors de la génération de pseudonymes.

*La disponibilité* peut être étudiée selon deux volets :

- Disponibilité à court terme : les données et les applications sont des ressources critiques qui doivent êtres disponibles aux utilisateurs autorisés après un temps d'attente raisonnable : pour le médecin en cas d'urgence, dans le cadre de la télégestion, où la gestion de l'état de santé du patient doit être immédiate alors qu'il s'agit d'échanger des données complexes comme des images ou des enregistrements de cardiogrammes.
- Disponibilité à long terme : le règlement des archives hospitalières impose des délais de conservation très longs : 70 ans pour les dossiers de pédiatrie, de neurologie, de stomatologie et de maladies "chroniques", illimités lorsqu'il s'agit de maladies héréditaires.

Par ailleurs, de nombreuses propriétés de sécurité peuvent être définies en termes de confidentialité, intégrité et disponibilité de l'information ou du service lui-même, ou encore de *méta-informations* comme l'instant de délivrance d'un service, ou de la réalisation d'une action ; l'identité de la personne qui a réalisé l'opération ; l'adresse d'une information, etc. [10, 11]. L'auditabilité correspond à la disponibilité et à l'intégrité de méta-informations relatives à l'existence d'une opération, à l'identité de la personne qui l'a réalisée, à l'instant de l'opération, etc. L'authenticité d'un message est équivalente à l'intégrité à la fois du contenu du message et de son origine. La non-répudiation correspond à la disponibilité et l'intégrité de l'identité de l'émetteur, l'instant de l'émission/réception, etc.

## 3 Politique et modèle de sécurité

L'analyse des politiques de sécurité et des modèles existants que nous avons effectuée dans [18, 19] permet de conclure que l'état de l'art actuel est insuffisant. En effet, le contrôle d'accès discrétionnaire (Discretionary Access Control) présente de sérieux inconvénients vis-à-vis des fuites d'informations et des chevaux de Troie, tandis que le contrôle d'accès obligatoire (Mandatory Access Control) [20, 21] est très rigide et mal adapté aux systèmes réellement répartis. La nature distribuée et inter-organisationnelle, ainsi que la diversité des scénarios des SICS, augmentent leur complexité.

La politique de sécurité que nous proposons dans [22] tient compte de ces caractéristiques et attribue les permissions selon :

- le rôle joué par l'utilisateur dans son organisation (infirmière dans l'unité de soins chirurgicale C5, médecin chef de l'hôpital de Rangueil, etc.) ;
- la relation de soin existante entre le professionnel de santé et le patient (le patient est traité/ à déjà été dans l'unité où le médecin fournit des soins) et/ou l'implication du professionnel de

santé au moment de la requête dans le processus de soins (l'accès entre dans le cadre d'un traitement du patient impliquant plusieurs organismes, le professionnel de santé appartient à l'un de ces organismes) ;

- d'autres informations contextuelles comme le lieu (adresse IP), le temps, l'urgence etc.

Avant d'accorder ou non un accès, le système doit, entre autres, récupérer les paramètres (identité, rôle, adresse IP, etc.) du demandeur, extraire les règle de sécurité concernées du serveur d'autorisation, et résoudre les conflits éventuels.

Le contrôle d'accès décide donc, à travers la politique de sécurité, si un utilisateur a le droit de réaliser une action donnée sur un objet donné. Le modèle HRU [23], par exemple, spécifie explicitement le triplet (sujet, objet, action) à travers une matrice de contrôle d'accès, où les lignes désignent les sujets, les colonnes désignent les objets et l'intersection d'une ligne et d'une colonne spécifie les droits du sujet sur l'objet ($M=(a_{ij})_{i\in Sujet\ ;\ j\in Objet}$). Néanmoins, pour les SICS, il est inconcevable que la politique de sécurité spécifie directement les droits associé à chaque utilisateur pour chaque objet. En effet, tout ajout ou suppression de sujet, d'objet ou d'objectif de sécurité nécessite une mise à jour directe de la politique de sécurité (ex : matrice de contrôle d'accès, règles de sécurité). D'autres part, cette mise à jour très fréquente de la politique de sécurité peut introduire des erreurs. Pour maîtriser la gestion de la politique de sécurité et réduire les erreurs d'administration, le modèle RBAC [24, 25, 26] décrit la politique de sécurité à travers des rôles. D'une part, les rôles sont associés aux utilisateurs, et d'autres part, les permissions (ensemble de droits) sont associées aux rôles. Un utilisateur obtient ainsi des droits selon le rôle qu'il joue dans le système. Cette manière de faire réduit les coûts dans la mesure où le rôle remplace l'ensemble de sujets qui réalisent la même fonction. Pour « N » utilisateurs jouant le même rôle au lieu d'éditer « N » règles, on en écrit une seule pour le rôle. En plus, l'ajout ou la suppression d'un utilisateur ne modifie que la relation (utilisateur, rôle) et non les règles de sécurité.

Le modèle ORBAC (Organization based-access control) que nous avons présenté dans [27] améliore RBAC et vise à résoudre certains problèmes rencontrés dans les systèmes multi-organisationnels, collaboratifs et dépendant du contexte.

Alors que RBAC est très générique, ORBAC raffine explicitement la structure des permissions. Dans ORBAC, une permission finale peut être vue comme un droit pour une action sur un objet.

ORBAC s'intéresse, non seulement aux permissions, mais aussi aux interdictions, obligations et recommandations.

ORBAC est centré autour de l'organisation (par exemple, l'hôpital, l'unité, le service). Même si un utilisateur a le droit de jouer plusieurs rôles, il n'a pas forcément le droit de les jouer dans toutes les organisations auxquelles il appartient. Le rôle peut différer d'une organisation à une autre. Et même la manière avec laquelle un rôle est perçu peut différer d'une organisation à une autre.

ORBAC distingue entre les entités du monde réel, utilisées au niveau du contrôle d'accès, et les entités abstraites utilisées au niveau de la politique de sécurité. Un rôle est une entité abstraite qui représente les utilisateurs ayant les mêmes fonctions. De la même manière, et afin de réduire les coûts et maîtriser la gestion et de la politique de sécurité au niveau des objets et des actions, nous ajoutons les entités abstraites « vue » et « activité ». L'ensemble des objets qui satisfont une propriété commune sont représentés à travers des vues et les actions qui réalisent les mêmes finalités sont représentées par des activités. La vue « dossiers médicaux » correspond pour une organisation X aux fichiers « *.doc » alors que pour une autre elle correspond aux fichiers du serveur Z ; l'activité « consultation » peut correspondre pour l'organisation X à l'exécution de l'action « Select » sur une base de donnée, tandis que pour Y, elle correspond à une action d'ouverture de fichier.

ORBAC est à la fois très flexible et très expressif. Il offre des possibilités d'héritage, de composition et de récursivité de ses concepts (équipes, groupes, organisations, processus). Dans ORBAC, il est par exemple possible d'attribuer des rôles (et donc des permissions), non seulement à des utilisateurs, mais aussi à des équipes. Il est également possible d'attribuer des droits sur des groupes composites d'objets. Par exemple, spécifier des permissions de réaliser des activités pour des rôles dans des organisations (utilisateurs de l'hôpital, qui eux-mêmes regroupés dans des équipes de soins) sur des vues (ou groupes d'objets) dans des organisations (les fichiers médicaux de l'unité C5).

Afin de réaliser un bon compromis entre le respect du principe du moindre privilège et la flexibilité du contrôle d'accès de façon à ne pas gêner le travail des personnels soignants, tout en respectant les droits des patients, nous pensons que toute action doit être inscrite dans l'un des deux cas suivants :

- soit dans un processus de soins impliquant le demandeur (membre d'une équipe impliquée dans le processus) et le patient (traité dans le processus) : l'activité de soins, initié par des

personnes habilitées (médecin traitant), est donc enregistrée dans le serveur comme activité en cours. Par exemple, un patient souffrant de douleurs abdominales peut se présenter chez son médecin traitant qui fera une première évaluation et initialise le processus de soins, avant d'envoyer le patient chez un spécialiste pour compléter et finaliser le diagnostic. Le patient reviendra enfin chez son généraliste pour assurer un suivi du traitement initié par le spécialiste. Le partage des données de santé de ce patient entre ces différents professionnels de santé s'effectue dans le cadre du processus de soins déclaré par le médecin traitant et constitué des trois plans de soins.

- soit en tant que cas exceptionnel. Dans le domaine médical, la vie des patients est prioritaire face à un contrôle d'accès. Ainsi une politique de sécurité rigide (cadrée par des processus bien définis) risque d'être rejetée par la communauté médicale. La solution que nous proposons est de prévoir des cas exceptionnels (en dehors des processus courants) où certains utilisateurs et/ou rôle peuvent déclarer un objectif précis (mais exceptionnel) de l'utilisation. La procédure repose sur deux types de contrôles :
    - Un contrôle en amont : les règles de sécurité doivent spécifier quel utilisateur/rôle a le droit de déclarer quel objectif, et dans quelles conditions. Par exemple l'objectif « urgence » peut être déclaré par un professionnel soignant si le médecin est absent (grève, force majeure, etc.). Il est important de noter que la finalité de l'activité à réaliser doit être clairement définie par le demandeur. Le système avertit alors l'utilisateur en engageant sa responsabilité, et lui attribue plus de permissions que d'ordinaire. Il renforce également les fonctionnalités d'audit et éventuellement envoi automatiquement une notification au patient ou au médecin traitant
    - un contrôle a posteriori, avec l'analyse des enregistrements d'audit, permettant de vérifier le bien fondé des décisions prises (par exemple, le caractère d'urgence).

Par exemple, on peut autoriser le médecin qui a traité autrefois un patient à ré-accéder à son dossier médical, à condition qu'il spécifie comme objectif pour cette utilisation : « révision du diagnostic, vérification ». Cet objectif (en plus du rôle) sera le point essentiel de l'autorisation et déclenchera automatiquement un audit (ou même l'envoi automatique d'une notification au patient).

# 4 Modèle formel

L'utilisation d'une approche formelle offre plusieurs avantages :

- assister l'administrateur à spécifier, définir et formaliser la politique de sécurité ;
- faciliter la tâche de dérivation des conséquences des risques et raisonner sur la réglementation en manipulant la spécification par des méthodes de calcul formel, par des outils de vérification et par d' autres outils de preuves automatiques ;
- bénéficier des fonctionnalités de la spécification logique, notamment : interroger la politique, vérifier les propriétés de complétude, vérifier si une situation viole la politique et vérifier si l'implémentation du système d'information, et en particulier des mécanismes de contrôle d'accès permet bien de garantir les propriétés de sécurité souhaitées, étudier les problèmes d'interopérabilités entre plusieurs politiques, ….

## *4.1 Langage formel proposé*

Le langage que nous avons présenté dans [22, 28], se base sur la logique déontique [29] qui ajoute aux opérateurs de la logique des prédicats ($\wedge$, $\vee$, $\neg$, $\Rightarrow$), des opérateurs modaux de permission **P**, d'obligation **O** d'interdiction **F** et de recommandations **R**. Les opérateurs déontiques de notre langage sont reliés par les relations suivantes (p est un prédicat) : $\mathbf{F}p = \mathbf{O}\neg p$ ; $\mathbf{P}p = \neg\mathbf{O}\neg p = \neg\mathbf{F}p$ $\mathbf{O}p \rightarrow \mathbf{R}p$ ; $\mathbf{R}p \rightarrow \mathbf{P}p$. Pour ne pas alourdir la présentation de ce formalisme dans cet article, nous n'expliquons que les grandes lignes de notre langage, les détails étant fournis dans [22, 28].

### 4.1.1 Alphabet du langage présenté

L'alphabet du langage présenté est constitué de constantes (entités), fonctions, variables, prédicats (associations) et actions. Les constantes, les variables et les fonctions de notre langage sont typées. Nous avons utilisé les types suivants : utilisateurs, rôles, équipes, unités, fichiers, données, etc.

Les constantes désignent les instances des entités de notre système, en l'occurrence les instances des utilisateurs, rôles, unités, fichiers, vues, patients, objectifs d'utilisations, etc.

Les variables désignent un élément quelconque représenté dans la politique de sécurité, par exemple : u∈*Utilisateurs*, r∈*Rôles*, éq∈*Équipe*, d∈*Donnée*.

Les fonctions servent à construire l'ensemble des termes du langage. Un dossier archive peut être exprimé par $DossierArchive(patient \times Fichier \times Fichier \times Fichier \times Fichier \times Fichier \times Fichier) \rightarrow Dossier$. Les arguments de cette fonction sont : identité du patient, résumé clinique, résumé infirmier, résumé psychiatrique, résumé gériatrique, résumé financier et résumé social. De la même manière, mais moins formellement, nous exprimons l'ensemble des données d'identité par la fonction « Données d'identité (nom et prénom, sexe, date de naissance, numéro de téléphone, nationalité) » et la CPS ou Carte de Professionnel de Santé par la fonction CPS (numéro d'identification, nom, profession, mode d'exercice, lieu d'exercice, tarification).

Les constantes, les variables et les fonctions sont les éléments de base qui permettent de définir les termes du langage ainsi que leur type par induction : toute constante ou variable est un terme ;

Si $f$ est une fonction de type $\lambda_1,..,\lambda_n \rightarrow \mu$ et si $t_1,..,t_n$ sont des termes de type $\lambda_1,..,\lambda_n$, alors $f(t_1,..,t_n)$ est un terme de type $\mu$. Par exemple, si GIP (groupement d'intérêt public) est une constante de type autorité, si Bob est un utilisateur, si CHU de Rangueil est de type établissement, si unité de chirurgie est de type unité, si bob@chu-toulouse.fr est de type adresse électronique, si A7:3F:..E1 est de type clé, si 29-09-2003 est de type date, si médecin est de type rôle et si 7C:C1::..C7 est de type clé, *Alors* le terme certificat électronique (GIP, Bob, CHU Rangueil, unité de chirurgie, bob@chu-toulouse.fr, A7:3F:..E1, 29-09-2003, médecin, 7C:C1::..C7) est un terme de type fichier qui dénote le certificat délivré par l'autorité GIP à l'utilisateur Bob au sein du CHU de Rangueil.

Après avoir défini les entités sous la forme de termes, il est naturel d'identifier les différentes relations qui peuvent exister entre ces entités. Ces relations sont dénotées par des prédicats. Par exemple, AUREq($u,r,éq$) : associe les rôles qu'un utilisateur peut jouer dans chacune de ses équipes.

Avec les prédicats, les actions définissent les éléments fondamentaux du langage. Par exemple : l'action LIRE($u,f$) correspond à la lecture du fichier par l'utilisateur.

### 4.1.2 Le langage

Au moyen des prédicats et des actions, on peut définir les formules atomiques : si A est un *prédicat* ou une *action* de type $\lambda_1,..,\lambda_n$ et si $t_1,..,t_n$ sont des termes de type $\lambda_1,..,\lambda_n$ alors $A(t_1,..,t_n)$ est une formule atomique. Par exemple, $AR(Bob,médecin)$ ; $LIRE(Bob,dossier_i)$. Le langage est généré par la règle de grammaire suivante, donnée en notation EBNF (Extended Backus Normal Form), où « f » désigne une formule : $f ::= A(t_1,...t_n) \mid \neg f \mid f \vee f \mid f \wedge f \mid \mathbf{O}f \mid \mathbf{P}f \mid \mathbf{F}f \mid \mathbf{R}f$

### 4.1.3 La sémantique

La sémantique utilisée est définie par le modèle $M = \langle W, \Re, V, D \rangle$ où

- $W$ est un ensemble de mondes possibles « $w$» ;
- $\Re$ est une relation d'accessibilité (relation binaire sur $W$) ;
- $D$ est un domaine . Un domaine est un ensemble non-vide de valeurs. Il est similaire à la notion de type que l'on trouve dans les langages de programmation.
- $V$ est une fonction qui donne les valeurs de vérité des éléments du langage : $V(w,A) \subseteq D^n$ ; $V(x) \in D$ ; $V(a) \in D$ ($A$ : formule atomique d'arité n, $x$ : variable et $a$ : constante).

Intuitivement, « (Bob, médecin) ∈ V(w,AR) » signifie que dans le monde $w$, $Bob$ joue le rôle *médecin* ; « (Sam,dossier$_1$) ∈ V(w,LIRE) » signifie que dans le monde $w$, $Sam$ exécute l'action « *LIRE* » sur le dossier « *dossier$_1$* ».

### 4.1.4 Conditions de vérité

$$M,w \models A(t_1,...t_n) \quad ssi \quad (V(t_1),...,V(t_n)) \in V(w,A)$$
$$M,w \models \mathbf{O}f \quad ssi \quad \forall w' \in W / w \Re w' \rightarrow M,w \models f$$
$$M,w \models \mathbf{P}f \quad ssi \quad \exists w' \in W / w \Re w' \rightarrow M,w \models f$$
$$M,w \models \mathbf{F}f \quad ssi \quad \forall w' \in W / w \Re w' \rightarrow (M,w \models \neg f)$$

Les opérateurs modaux permettent de modifier les propriétés de la relation « $\Re$ » entre les différents mondes du modèle associé à la spécification. Ils indiquent si deux mondes doivent ou non être accessibles l'un depuis l'autre. Les formules $\mathbf{O}f$, $\mathbf{P}f$ et $\mathbf{F}f$ signifient respectivement : à partir de n'importe quel monde accessible, on doit pouvoir atteindre un monde dans lequel $f$ est vraie ; on doit pouvoir atteindre un monde dans lequel $f$ est vraie ; aucun des mondes accessibles ne doit permettre de conclure que $f$ est vraie dans ce monde.

## 4.2 Spécification de la politique de sécurité dans ce langage

L'étude formelle de la fonction de sécurité nécessite, tout d'abord, la représentation des règles de fonctionnement les plus pertinentes vis-à-vis de la sécurité, les besoins de sécurité (les différentes formes que peuvent prendre la confidentialité, l'intégrité et la disponibilité dans les SICS) ainsi que les règles de sécurité (ex : dans quelles conditions, un médecin a le droit d'accéder à un fichier médical).

### 4.2.1 Règles de fonctionnement

Le but de la spécification des règles de fonctionnement et des règles de sécurité est de définir les différents flux d'informations et les contrôles de sécurité afin de pouvoir, ultérieurement, déterminer l'impact sur les besoins de sécurité. La description se fait par le biais des opérateurs de la logique propositionnelle. Au niveau de la sémantique, les règles de fonctionnement définissent la structure interne des mondes associé à la spécification. Ce sont en effet, des axiomes ne contenant pas d'opérateurs modaux. Ils n'ont donc aucun impact sur les caractéristiques de la relation $\Re$ entre les mondes du modèle. En revanche, chaque monde est tel qu'il constitue un état de fait compatible avec les règles de fonctionnement. Ainsi, la règle $q \rightarrow r$ signifie : dans tout monde $w$ où $q$ est vraie, $r$ l'est aussi. $\mathrm{AR}(x, \mathit{Médecin}) \vee \mathrm{AR}(x, \mathit{PersInfirmier}) \vee \mathrm{AR}(x, \mathit{AideSignante}) \rightarrow \mathrm{AR}(x, \mathit{PersSoignant})$ signifie que si x est un médecin, un personnel infirmier ou une aide-soignante alors il est personnel soignant.

### 4.2.2 Objectifs de sécurité

Les objectifs de sécurité sont exprimés en utilisant les opérateurs modaux. Ces opérateurs permettent de modifier les propriétés de la relation d'accessibilité $\Re$ entre les différents mondes du modèle. Ils indiquent si deux mondes doivent être accessibles l'un depuis l'autre. La règle $\mathbf{F}[\mathit{AR}(u, \mathit{pharmacien}) \wedge \mathtt{CREER}(u, \mathit{ordonance}(\_,\_,\_,\_))]$ interdit au pharmacien de créer des ordonnances.

### 4.2.3 Règles de sécurité

Du point de vue formel, une règle de sécurité est une formule modale dont les différentes clauses ne sont pas toutes des formules modales, par exemple $r \rightarrow \mathbf{P}q$. Dans ce cas, la règle précise une relation logique entre l'état existant dans un monde et les règles déontiques qui s'appliquent. $\mathrm{ADoss}(p, \mathit{dossier}_i) \rightarrow \mathbf{P}[\mathtt{LIRE}(p, \mathit{dossier}_i)]$ exprime une des règles de la loi [8] et du décret [9] qui autorise à un patient de lire son dossier médical *« toute personne a accès à l'ensemble des informations concernant sa santé… »*.

## 4.3 Vérification de la politique de sécurité

La spécification formelle que nous venons de présenter peut être exploitée sous différents aspects et détecter différents types d'incohérences :

- Étant donné que les règles de sécurité permettent de savoir comment un état de sécurité évolue, et que les objectifs de sécurité permettent de savoir si un état est sûr, il peut être souhaitable de vérifier qu'il n'est pas possible, partant d'un état initial sûr, d'atteindre un état non sûr (en appliquant les règles de sécurité).
- Vérifier si les objectifs de sécurité ne sont pas contradictoires entre eux. Par exemple, exclure le cas où une obligation et une interdiction sont en conflit revient à vérifier que $\neg(\mathbf{O}q \wedge \mathbf{F}q)$ est vraie pour la spécification effectuée.
- Vérifier si la dérivation des règles de sécurité ne mène pas à une contradiction. Par exemple, un utilisateur confronté à une interdiction et à une obligation de faire la même action.
- Vérifier si les règles de fonctionnement ne peuvent jamais entrer en conflit avec les besoins et les règles de sécurité qui ont été définis.

- Associer un des axiomes de la logique déontique à la spécification. Par exemple, l'axiome D « $\mathbf{Op} \Rightarrow \mathbf{Pq}$ » correspond à la volonté d'inclure qu'une obligation doit impliquer la permission correspondante, ce qui signifie que la relation d'accessibilité $\Re$ possède la propriété : $\forall w, \exists w' \mid w \Re w'$.

Différentes approches peuvent être utilisées pour effectuer des calculs (vérifications) dans un langage modal. Nous optons pour l'utilisation de la méthode des tableaux [30] qui consiste, pour prouver une formule f, à faire l'hypothèse ¬ f et à dériver une contradiction en scindant successivement f et chacune de ses sous-formules jusqu'à ce que l'on obtienne à la fois une formule et sa négation. Le choix de cette méthode est justifié par les informations qu'elle fournit sur l'échec ou le succès de la démonstration. Notamment, dans le cas où un objectif de sécurité n'est pas vérifié, il est primordial de pouvoir en expliquer la raison et donc de détailler l'état ou la succession d'états qui est à l'origine de l'échec. Un exemple de vérification d'une politique de sécurité par cette méthode est donné dans [31].

# 5 Mise en œuvre

Notre politique de sécurité ainsi spécifiée et vérifiée peut être implémentée par différents mécanismes de contrôle d'accès. En particulier, dans le cadre du projet MAFTIA (Malicious – and Accidental fault tolérance in Internet Applications), le LAAS – CNRS [32] a développé des mécanismes de délégation sophistiqués respectant le principe du moindre privilège et qui ne présentent pas les inconvénients des schémas d'autorisation basés sur un modèle client-serveur. Le schéma se base sur un moniteur de référence, composés d'un objet Java spécifique, le dispatcher, et d'un noyau de sécurité implémenté dans une carte à puce Java. Le moniteur de référence a la responsabilité de contrôler les accès aux objets situés sur la machine locale. Il permet de vérifier, par des mécanismes cryptographiques, que les capacités accompagnant les invocations autorisent bien l'appel des méthodes des objets locaux. Pour réaliser une action donnée, le système accorde à l'utilisateur des droits (sous forme de capacités) dont certains (les coupons) ne sont pas directement utilisables par l'utilisateur mais délégués à d'autres objets du système. Il est également envisageable d'implémenter la politique de sécurité à l'aide de langages interprétés tel que XML (eXtensible Markup Language) qui permet d'échanger les informations via le web tout en fournissant un contrôle d'accès tenant compte de la structure et du contenu sémantique des documents. [33] explique comment peut ont exploiter XML pour fournir un contrôle d'accès adapté à notre système.

Par ailleurs, les techniques de tolérance aux fautes classiques peuvent renforcer nos dispositifs de sécurité. La réplication permet de se protéger contre les modifications et les destructions non-autorisées (disponibilité et intégrité). Le chiffrement permet de se protéger contre les écoutes passives, comme l'acquisition de messages sur un réseau ou l'accès à des informations stockées. La signature cryptographique permet de détecter des modifications non-autorisées. Le brouillage consiste à ajouter des informations superflues ou à augmenter l'incertitude dans les réponses aux requêtes statistiques dans les bases de données pour tolérer les attaques par inférence. La technique de Fragmentation-Redondance-Dissémination permet de renforcer à la fois la confidentialité, l'intégrité et la disponibilité. Cette technique consiste à découper l'information en fragments de telle sorte que des fragments isolés ne puissent fournir d'information significative, à ajouter de la redondance pour empêcher que la modification ou destruction de quelques fragments ait des conséquences pour les utilisateurs autorisés, puis à isoler les fragments les uns des autres par dissémination de sorte qu'une intrusion dans une partie du système ne fournisse que des fragments isolés. Il est parfois nécessaire de faire appel à des techniques de *détection et recouvrement des intrusions* [2] pour :

- détection des intrusions, par les mécanismes de contrôle d'accès, complétés par des dispositifs permettant de discriminer entre le comportement normal des utilisateurs autorisés et un comportement anormal qui peut être le signe d'une intrusion ; ces dispositifs de discrimination peuvent être basés sur une comparaison avec une référence du comportement normal ou sur une reconnaissance d'un comportement anormal connu (signature d'attaque) ;
- ralentir des intrusions, soit en combattant l'intrus par la résiliation des droits qu'il a pu obtenir soit en le trompant ou en lui fournissant des informations inutiles
- intervenir par la localisation de l'intrus et les poursuites judiciaires à son encontre, et par la restauration éventuelle des informations détruites et la correction des failles de sécurité.

# 6 Conclusion

Ce papier a présenté une démarche globale de sécurisation de systèmes complexes, distribués et multi organisationnels, à travers une étude de cas dans les systèmes d'information et de communication de santé. Il s'est appuyé sur les textes juridiques pour identifier les informations à protéger, caractériser les menaces et décrire les besoins de sécurité. Ensuite, il décrit comment le modèle de sécurité ORBAC améliore le modèle RBAC et attribue les permissions/obligations/recommandations/interdictions pour réaliser des activités à un rôle dans une organisation, sur un groupe d'objets dans un contexte donné. Le papier a également expliqué certains mécanismes de sécurité et de sûreté de fonctionnement susceptibles d'implémenter la politique de sécurité ainsi que des méthodes pour vérifier cette politique.

Nous envisageons d'enrichir notre politique et modèle de sécurité pour satisfaire des besoins élevés de propriétés de sécurité (en particulier de disponibilité), de finaliser le cadre réglementaire, d'intégrer d'autres concepts comme la délégation et de vérifier la cohérence de la politique de sécurité. La suite des travaux consistera également à compléter l'implémentation à l'aide des mécanismes de sécurité décrits, avant de préparer un processus d'évaluation et de certification au sens des critères d'évaluation de la sécurité des systèmes d'informations (Critères Communs : ISO/IEC 15408).

# 7 Remerciements

Cette étude est partiellement soutenue par le Réseau National de Recherche en Télécommunications (RNRT) dans le cadre du projet MP6 (*Modèles et Politiques de Sécurité pour les Systèmes d'Informations et de Communications en Santé et Social*), dont les partenaires sont : Ernst & Young Audit, ENST-Bretagne, ETIAM, France Telecom R&D, LAAS-CNRS, MasterSecuritY, ONERA-DTIM, Supélec-Rennes, UPS-IRIT. Elle entre également dans le cadre des travaux du projet « Sécurité Informatique » de FéRIA, la Fédération de Recherche en Informatique et Automatique de Toulouse. Les auteurs remercient en particulier Philippe Balbiani de l'IRIT pour sa contribution importante à la formulation du langage.

# Références

[1] ITSEC, *Critères d'évaluation de la sécurité des systèmes informatiques*, v1.2, 163p., ISBN 92-826-3005-6, Office des publications officielles des Communautés Européennes, Luxembourg, 1991.

[2] J.-C. Laprie, J.Arlat, J.-P. Blanquart, A. Costes, Y. Crouzet, Y. Deswarte, J.-C. Fabre, H. Guillermain, M. Kaâniche, K. Kanoun, C. Mazet, D. Powell, C. Rabéjac et P. Thévenod, *Guide de la sûreté de fonctionnement*, 324p., Edition Cépaduès, ISBN : 9782854283822, Toulouse 1995.

[3] A. Abou El Kalam, P. Balbiani, S. Benferhat, L. Veyssiere, F. Cuppens, Y. Deswarte, R. El-Baida, F. Nambot, C. Saurel, G. Trouessin, *Informations à protéger et menaces*, Projet MP6, sous-projet 3 : Politiques de sécurité pour les SICSS. Rapport LAAS N° : 02334, septembre 2002, 34p.

[4] La résolution A/RES/45/95 L'Assemblée générale des Nations Unies : "*Principes directeurs pour la règlementation des fichiers personnels informatisés*„ 14 December 1990.

[5] Recommandations du Conseil de l'Europe, R(97)5, *on The Protection of Medical Data Bank*s, Council of Europe, Strasbourg, 13 février 1997.

[6] Draft Recommendation of the Communication of Health Information in Hospitals, European Health Commitee CDSP (92)8, Council of Europe, Strasbourg, 21 juin 1992.

[7] Directive du parlement Européen du Conseil, adoptée par le Conseil le 24 juillet 1995 : « *On the protection of individuals with regard to the processing of personnal data and on the free movement of such data* » ; 1995.

[8] Loi 2002-303 du 4 mars 2002 relative aux *droits des malades et à la qualité du système de santé*.

[9] Décret 2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenus par les professionnels et les établissements de santé en application des articles L.1111-7 et L.1112-1.

[10] D. Powell et R. Stroud (Eds.), *Malicious and Accidental-Fault Tolerance in Internet Applications: conceptual model and architecture*, Livrable D2 du projet MAFTIA, Novembre 2001.

[11] A. Abou El Kalam, Y. Deswarte, D. Powell, Livrable : *Concepts et terminologie génériques*, Projet MP6 : Politiques de sécurité pour les SICSS. Rapport Laas Rapport LAAS N° : 02268, Juillet 2002, 19p.

[12] Directive du Parlement Européen N° : 2002/58/EC concernant "*le traitement des données à caractère personnel et la protection de la vie privée dans le secteur de télécommunications électroniques*„, 12 juillet 2002, Journal Officiel L 201, 31-7-2002, p. 37-47.

[13] B. Woodward, "The computer-based patient record and confidentiality„, *New England Journal of Medicine*, v 333 N° 21, 1995, pp 1419-1422.

[14] Audit Commission, *Ghost in the* Machine - An Analysis of IT Fraud and Abuse, Audit Commission Publications, United Kingdom, ISBN 1-86240-05603, 1998.

[15] Code de déontologie médicale, décret 95-1000 du 6 septembre 1995

[16] Code de la santé publique, code de la famille et de l'aide social.Paris :Dalloz 1995

[17] Tufo, H.M., and J.J. Spiedel. Problems with médical records. Medical Care 9 :509-517 ; 1971.

[18] A. Abou El Kalam, Y. Deswarte, "Contrôle d'accès basés sur les rôles, les groupes d'objets et le contexte : Étude de cas dans les Systèmes d'information et de Communication en Santé„, *Sécurité et Architecture des Réseaux (SAR'02)*, Marrakech, 8-12 juillet 2002, 11p.

[19] A. Abou El Kalam, "Politiques de sécurité pour les systèmes d'informations médicales„, *Journées Doctorales en Informatique et Réseaux (JDIR)*, Toulouse, France, 4-6 mars 2002, pp 201-210.

[20] D.E.Bell, L.J.LaPadula, *Secure Computer Systems : Unified Exposition and Multics Interpretation*, The MITRE Corporation, TechnicalReport, ESD-TR-73-306, 1975.

[21] K.J.Biba, *Integrity Consideration for Secure Computer Systems*, The MITRE Corporation, Technical Report, ESD-TR-76-372 & MTR-3153, 1977.

[22] A. Abou El Kalam, Y. Deswarte, "Security model for Health Care Computing and Communication Systems„, *18th IFIP International Information Security Conference (SEC'03)*, Athènes, 26-28 Mai 2003.

[23] M.A. Harrison, W.L. Ruzzo et J.D. Ullman, Protection in Operation Systems, *Communication of the ACM*, 19(8) : 461-471, oût 1976.

[24] R. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, "Role-Based Access Control Models„, IEEE Computer, vol.29, pp.38-47, février 1996.

[25] S.I. Gavrila, J.F. Barkley "Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management„, *Third ACM Workshop on Role-Based Access Control*, Fairfax, VA, USA. 22-23 octobre 1998.

[26] D.F. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn and R. Chandramouli "A Proposed Standard for Role-Based Access Control„, *ACM Transactions on Information and System Security*, V 4, N° 3, août 2001.

[27] A. Abou El Kalam, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, R. El-Baida, A. Miège, C. Saurel, G. Trouessin "Organization-Based Access Control„, *IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy'03)*, Lake Como, Italie, 4-6 juin 2003. Rapport Laas N° : 02590, décembre 2002, 13p.

[28] A. Abou El Kalam, Y. Deswarte, Modèle de sécurité pour le secteur de la santé, soumis à *Technique et Science Informatique (TSI)*. Disponible sous Rapport LAAS N°02433.

[29] B.F. Chellas, *Modal Logic: An Introduction*, 295p., Cambridge University Press, 1980, ISBN 0-521-29515-7.

[30] L. Farians del Ceddo, A. Heriz, Modal Deduction with apllications in Epistemic and Temporal Logic, in *Handbook of Logic in Artificial Intelligence and Logic Programming*, vol. 4/5, pp. 499-594, ISBN0-19-853791-3, Oxford Science Publications, 1995.

[31] R. Ortalo, *Evaluation quantitative de la sécurité des systèmes d'information*, Thèse de doctorat, Institut National Polytechnique de Toulouse, 1998. Rapport Laas N° : 98164.

[32] Y. Deswarte, N. Abghour, V. Nicomette, D. Powell, "An Intrusion-Tolerant Authorization Scheme for Internet Applications„, *in Sup. of the Proceedings of the 2002 International Conference on Dependable Systems and Networks (DSN2002)*, Washington, D.C. (USA), 23-26 June 2002, pp. C-1.1 - C-1.6.

[33] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, "A Fine-Grained Access Control System for XML Documents„, *ACM Transactions on Information and System Security*, V 5, N° 2, May 2002.