Modèles et politiques de sécurité des systèmes d'information et de communication en santé et en social

Anas Abou El Kalam, Philippe Balbiani, Salem Benferhat, Frédéric Cuppens, Yves Deswarte, Rania El-Baida, Claire Saurel, Gilles Trouessin

Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication en Santé et Social

Anas Abou El Kalam *, Philippe Balbiani**, Salem Benferhat**, Frédéric Cuppens***,
Yves Deswarte *, Rania El-Baida**, Claire Saurel***, Gilles Trouessin****

* LAAS-CNRS. 7 avenue du colonel Roche. 31077 Toulouse Cedex 4 .{Yves.Deswarte, anas}@laas.fr
** IRIT – 118, route de Narbonne. 31062 Toulouse Cedex 4. {benferhat, elbaida, balbiani}@irit.fr
*** ONERA Centre de Toulouse - BP 4025 - 31055 Toulouse Cedex {cuppens, saurel}@cert.fr
**** ERNST & YOUNG - 1, place Alfonse Jourdain – 31000 Toulouse, gilles_trouessin@ernst-young.fr

Résumé

Cet article présente des travaux menés dans le projet MP6[1]. Il montre comment, compte tenu de la sensibilité des informations manipulées, les Systèmes d'Information et Communication en Santé et Social (SICSS) peuvent être convoités par des individus malintentionnés. Sont alors présentés les objectifs de MP6 face au besoin crucial de sécurité informatique, dans un domaine où la dynamicité des contextes d'exploitation et la complexité organisationnelle des organismes utilisateurs excluent des solutions développées dans d'autres secteurs, comme la défense ou la banque. MP6 vise notamment à définir un outil d'assistance à l'élaboration de politiques de sécurité pour les SICSS : cet outil doit permettre à l'utilisateur (par exemple un médecin DIM[2]) d'exprimer une politique sous la forme d'un ensemble de règles, puis de vérifier qu'elle respecte des propriétés attendues (disponibilité, intégrité, confidentialité, auditabilité, etc.). L'article présente un ensemble de concepts nécessaires pour exprimer une politique de sécurité tenant compte des spécificités des mondes santé et social. Il montre enfin comment la capacité expressive et le mécanisme déductif de certaines logiques non classiques permettent de décrire formellement une telle politique de sécurité et de calculer automatiquement si elle vérifie les propriétés de sécurité souhaitées.

Mots clés

Systèmes d'informations médicaux, sécurité des systèmes d'information, protection des données à caractère personnel, politiques de sécurité, secteur santé et social

[1] Modèles et Politiques de Sécurité pour les Systèmes d'Informations et Communications en Santé et Social

[2] département d'informatique médicale

1. Problèmes de sécurité concernant les SICSS

1.1 Définition et enjeux des SICSS

Les Systèmes d'Informations et de Communication dans les secteurs Santé et Social (SICSS) permettent de stocker et gérer des informations médicales, administratives ou sociales concernant des individus. Ils doivent faciliter les tâches de leurs utilisateurs médecins, secrétaires médicaux, infirmiers, ou encore agents d'assurances maladie, tous en charge de traitements à effectuer pour ces individus (diagnostics, actes médicaux, soins, remboursements…). Ces systèmes manipulent entre autres des données à caractère personnel et souvent nominatives - contribuant à la description d'individus bien identifiés ou identifiables; citons les informations décrivant, pour un patient, ses situations médicales (historique et situation actuelle des pathologies et allergies, diagnostics, actes médicaux, résultats biologiques), administratives (identité et coordonnées, situation familiale) ou sociales (prestations financières et sociales).

Les SICSS exploitent la puissance et les progrès des technologies de l'informatique et des réseaux pour permettre aux utilisateurs un accès rapide à ces informations, et ainsi faciliter et contrôler la prise en charge médicale, administrative ou sociale des patients, assurés ou bénéficiaires. Toutefois la mise en œuvre de telles technologies met en péril l'intimité des données gérées par les SICSS. En effet, le marché des informations nominatives attire de nombreuses convoitises : industries pharmaceutiques, compagnies d'assurances, assurance maladie, banques, employeurs, presse, stratèges politiques. Les SICSS sont donc des cibles précieuses pour des individus malintentionnés, susceptibles d'exploiter toute vulnérabilité du système pour violer les propriétés de *confidentialité* (non divulgation d'information sensible à des personnes non autorisées à la connaître), *intégrité* (non altération d'information sensible), *disponibilité* (fourniture de l'information à qui de droit, dans les délais prévus en fonction du droit du demandeur de l'information) ou *auditabilité* (garanties de traçabilité, d'imputabilité et d'opposabilité des actions effectuées dans le système).

1.2 Menaces pesant sur les informations manipulées par ces systèmes

Citons seulement quelques risques liés à l'utilisation de l'informatique puis de la télématique (Abou el Kalam, 2002). L'exploitation abusive par un utilisateur malhonnête d'un SICSS insuffisamment protégé peut permettre la divulgation de données personnelles intimes. La peur d'un manque de confidentialité de tels systèmes peut dès lors inciter des patients à refuser de divulguer des informations pourtant vitales pour eux. Des erreurs de saisie de données ou de conception dans un SICSS peuvent entraîner des erreurs de diagnostic ou d'actes médicaux. L'implantation d'un SICSS dans un lieu mal protégé, les défaillances ou sabotages peuvent rendre inaccessibles des informations aux médecins qui peuvent en avoir besoin pour leurs patients ou pour justifier leurs décisions si nécessaire.

D'un point de vue télématique, la connexion des SICSS à un réseau multiplie le risque d'intrusions, de divulgation du contenu sensible de messages électroniques, et de croisement d'informations non désirable entre divers secteurs (par exemple, médical et assurance). Elle ouvre la porte à des virus susceptibles de modifier ou détruire tout ou partie du système et son contenu. L'utilisation de technologies liées à Internet induit des vulnérabilités et des risques de malveillance pour les sites visités ou visiteurs. Enfin, le manque de confiance peut conduire chaque partenaire d'un SICSS à installer sa propre politique de sécurité, au détriment d'une interopérabilité pourtant indispensable à l'échange nécessaire d'informations.

2 Objectifs du projet MP6 pour la sécurité des SICSS

2.1 Fondements de MP6

MPSSICSS (ou MP6[3]) est un projet[4] de *Recherche et Développement* consacré à la sécurité des SICSS. Il est destiné à mener des investigations et à proposer des axes de pré-industrialisation, autour de risques répertoriés et de menaces émergentes pour les SICSS, afin de leur procurer les protections et parades nécessaires à une sécurité optimale. Ces dernières années, plusieurs projets européens (ISHTAR, TrustHealth, DIABCARD, MedSec, Harp, EUROMED-ETS, HANSA, PRIDEH et DRIVE) se sont penchés sur les problèmes de sécurité des SICSS. Certaines études ont porté en particulier sur les cartes à puces, les mécanismes bio-métriques et les infrastructures de gestion de clés. Au niveau des politiques et modèles de sécurité, les résultats sont encore insuffisants.

2.2 Origines de MP6

Certaines des principales interactions entre applications ou systèmes peuvent être très exigeantes en matière de sécurité - *disponibilité*, *intégrité*, *confidentialité* et *auditabilité* - des systèmes d'information et de communication, ce qui permet d'intégrer les *devoirs* et *pouvoirs* et les *obligations* ou *interdictions* attribués à chacun des acteurs et issus des responsabilités qu'ils doivent endosser ou exercer. Ceci est particulièrement vrai dans les différents secteurs de la sphère Santé-Social, notamment pour le respect de la vie privée et la protection des données à caractère personnel (Trouessin, 2001).

Des mécanismes classiques (authentification, autorisation, contrôle d'accès, chiffrement réversible, signature numérique) existent tant au niveau des réseaux pour fournir la sécurité nécessaire des communications à protéger, qu'au niveau des systèmes informatiques pour apporter et garantir la sécurité des systèmes manipulant des informations sensibles.

2.3 Finalités de MP6

Pour leur mise en œuvre efficace, il est indispensable de définir précisément les besoins de sécurité des utilisateurs -"propriétés de sécurité"- , les règles de sécurité à appliquer et les priorités à appliquer en cas de conflits entre ces règles -"modèles de politiques de sécurité"-. MP6 s'attache ainsi à prendre en compte les concepts sectoriels particuliers, tels l'auditabilité juridico-technique (Trouessin, 2002) issue des responsabilités juridiques spécifiques (légales-réglementaires, éthiques-déontologiques, médicales, sociales), pour élaborer les propriétés de sécurité à garantir, les politiques de sécurité à respecter et les modèles de sécurité adaptés et adaptables aux SICSS. MP6 vise à améliorer la pertinence, l'efficacité des systèmes des secteurs ciblés et la confiance à accorder à de tels systèmes. MP6 aborde plusieurs problématiques de recherche: politiques de sécurité et modèles de politiques de sécurité, politiques d'autorisation, d'anonymisation et de non-inférence illicites. L'objectif de MP6 abordé dans cet article concerne la définition d'un outil d'assistance à l'élaboration de politiques de sécurité pour les SICSS: cet outil doit permettre à l'utilisateur (par exemple un médecin DIM) d'exprimer une politique de sécurité sous la forme d'un ensemble de règles, puis de vérifier si la politique ainsi définie vérifie des propriétés attendues (assurance de confidentialité, disponibilité, intégrité, auditabilité, etc.).

---

[3] MP6: Modèles et Politiques de Sécurité pour les Systèmes d'Information et de Communication en Santé et Social

[4] MP6 est un projet financé dans le cadre du programme RNRT lancé par la Direction des Technologies au Ministère de la Recherche. MP6 rassemble neuf partenaires (Ernst&Young Audit, LAAS-CNRS, IRIT-UPS, ONERA-Toulouse, Master Security, ENST Bretagne, Supélec et France Télécom R&D), issus tant de la recherche, du développement, que du management ou développement de projets en sécurité des systèmes.

3 Concepts de base

Pour définir un langage d'expression d'une politique de sécurité adaptée aux caractéristiques du secteur santé-social, il faut se donner un ensemble pertinent de concepts de base à utiliser pour énoncer cette politique. Les concepts suivants ont été retenus après étude de l'état de l'art approprié.

3.1 Les modèles classiques de politiques de sécurité

L'analyse des politiques de sécurité et des modèles existants (Abou el Kalam, 2002; Abou el Kalam et Deswarte, 2002) permet de conclure que les systèmes de contrôles d'accès existants sont insuffisants . En effet, le contrôle d'accès discrétionnaire[5] («Discretionary Access Control», ou DAC, en anglais) présente de graves inconvénients vis-à-vis des fuites d'informations et des chevaux de Troie, tandis que le contrôle d'accès obligatoire[6] («Mandatory Access Control», ou MAC) (Bell et LaPadula, 1975) est très rigide et mal adapté aux systèmes réellement répartis. La motivation initiale de cette étude est de fournir, aux SICSS, une politique de contrôle d'accès réalisant un bon compromis entre MAC et DAC,en assurant simultanément la sécurité et la flexibilité du contrôle d'accès.

3.2 Le contrôle d'accès basé sur les rôles

Une politique où les droits d'accès sont attribués à l'utilisateur en fonction du rôle qu'il joue dans le système d'information est appelée politique par rôle (Sandhu *et al*., 1996; Gavrila et Barkley,1998). Un rôle désigne une entité intermédiaire entre utilisateurs et privilèges (ensembles de droits). Les rôles permettent de faciliter l'administration de la politique de sécurité et de réduire les coûts de gestion des droits d'accès. Néanmoins, ce concept général doit être complété pour satisfaire tous les besoins des SICSS en termes de contrôle d'accès. L'un des problèmes principaux est que, dans une politique basée sur les rôles, tous les utilisateurs ayant le même rôle ont les mêmes privilèges. Or, par exemple, seul le médecin traitant peut consulter le dossier médical d'un patient. Autrement dit, tous les utilisateurs ayant le même rôle n'ont pas les mêmes privilèges. Les privilèges doivent donc être attribués, non seulement selon le rôle, mais aussi selon: la relation de soin existante entre le professionnel de santé et le patient; l'implication du professionnel de santé dans le processus de soins; d'autres informations contextuelles: lieu, temps, urgence, etc. En effet, la loi précise que l'accès à tout ou partie d'un dossier médical est fondamentalement conditionné par le statut de«*personne soignante, actuellement en charge du patient. Il est limité aux données dont la connaissance est nécessaire pour l'administration des soins et pendant la durée de ceux-ci*» (BCN 84, 1998). C'est dans cette logique et afin d'offrir un contrôle d'accès plus adapté, que nous introduisons le concept de groupe d'objets.

3.3 Concept de groupe d'objets

La suite de l'article tiendra compte du partitionnement classique des éléments du système en deux grandes catégories: les *sujets* sont des entités actives (utilisateurs) qui manipulent l'information, et les *objets* sont des entités passives (fichiers), contenant de l'information, sur lesquelles les sujets effectuent des actions. Selon l'action en cours, un même élément peut être sujet (un patient qui consulte son dossier médical) et objet (le même patient auquel une infirmière fait une injection). La spécification peut identifier des classes d'objets: équipements, dossiers, etc. Néanmoins, du point de vue du contrôle d'accès, cette classification est insuffisante et il faut distinguer les objets passifs de la même classe, sur

5. Une politique est dite discrétionnaire si l'entité qui possède un objet peut propager et manipuler librement les droits sur cet objet. Par exemple, la gestion des accès aux fichiers du système d'exploitation UNIX suit une politique discrétionnaire.

6. Les politiques obligatoires décrètent des règles incontournables, par exemple, en affectant aux entités, des attributs (des niveaux) qui ne sont pas modifiables par les usagers, et donc qui limitent leur pouvoir de gérer les accès.

lesquels les sujets peuvent avoir des droits différents ; d'où l'idée de construire des groupes d'objets selon des critères liés aux droits d'accès. Par exemple : le groupe Gd_i désigne les dossiers « $Doss_{i1}$,..., $Doss_{in}$ » traités par l'équipe *i* ; le groupe Gd_j désigne les dossiers « $Doss_{j1}$,.., $Doss_{jk}$ » traités par l'équipe *j*. Les deux dossiers $Doss_{in}$ et $Doss_{jk}$ sont tous les deux instances de la classe *dossier*, mais ils appartiennent à deux groupes différents. La construction des groupes d'objets se fait en trois étapes :

Première étape : selon une vue *logique*, effectuer des *regroupements* d'objets (dossiers des patients traités par un médecin donné, ressources d'une unité de soins) de façon à faire des distinctions entre les objets sur lesquels différents groupes de sujets effectuent différentes actions[7]. Dans les SICSS, la construction des groupes doit posséder une sémantique. Elle regroupe les objets selon des critères comme : l'appartenance à un hôpital, à une unité, à un projet, à une tâche de soins, etc. Par exemple, nous pouvons considérer les ressources d'une unité de soins (ou d'une équipe ou d'un médecin) comme deux groupes d'objets associés à cette unité de soins (ou à l'équipe ou au médecin).

Deuxième étape : relier chaque groupe avec les actions effectuées sur les objets qui le constituent. Une des manières de faire est de regrouper les objets sur lesquels sont effectuées les mêmes actions. Ainsi, en jouant un rôle donné, l'utilisateur obtient des privilèges lui permettant de réaliser des actions, non pas sur tous les objets d'une classe, mais sur une partie désignée par le groupe mentionné.

Troisième étape : réduire la complexité et améliorer la structuration à travers l'héritage de classes d'objets (par exemple : la ressource de l'unité de chirurgie ***est une*** ressource d'une unité de soins) ou la composition de groupes d'objets (par exemple : ressource de « l'équipe C_5 » ***est composée de*** deux salles, de dix ordinateurs et des dossiers de spécialité des patients ayant transité par cette unité).

Outre les raisons de structuration, les groupes d'objets sont construits pour établir le lien entre les sujets (professionnels de santé) et les objets qu'ils manipulent (fichiers des patients qu'ils traitent), au moyen d'actions. Par ailleurs, les *entités de structuration* (rôles, classes et groupes d'objets), ainsi que *les associations* {Rôle, Privilège}, {Privilège, action} et {action, groupe} restent relativement fixes dans le système d'information ; elles sont donc gérées par l'administrateur. En revanche, l'association {objets, groupe}, par exemple (Marie, patiente à l'unité de chirurgie C_5), change plus souvent, elle peut donc être gérées localement (l'affectation des patients aux unités de soins se fait par le personnel d'accueil de l'hôpital). Ainsi, ce nouveau concept contribue à *réduire les erreurs d'administration*. D'autre part, *les coûts d'administration* sont également réduits. En effet, les relations d'héritage et de composition favorisent la propagation des valeurs d'attributs des sous-classes vers les super-classes, et les actions sur l'agrégat vers les composants. En plus, le coût des associations {action, objet} (sans passer par le groupe) est de l'ordre de « N_A*N_O, tel que N_A est le nombre d'actions et N_O est le nombre d'objets ». Alors qu'en passant par un groupe, le coût est « N_A+N_O », et ceci pour chaque groupe.

3.4 Notion d'équipe

L'équipe est une entité regroupant un ensemble d'utilisateurs ayant différents rôles[8] et qui collaborent pour réaliser une tâche de soins. Dans la pratique une équipe est généralement associée à une organisation (hôpital, service, unité). Il est possible de mettre des contraintes sur la construction des équipes, en particulier des contraintes de cardinalité du type : une équipe peut être constituée d'au moins/au plus *N* utilisateurs ; dans une équipe, il faut au moins/au plus *N* utilisateurs ayant le rôle *r*. Par ailleurs, la propriété de responsabilité, imposée par la (Conseil de l'Europe, 1981), peut être intégrée au niveau des équipes. En effet, cette loi exige que *le responsable d'un fichier s'engage à prendre toute*

7. Dans UNIX par exemple, les fichiers qui appartiennent au même groupe d'utilisateurs ont des identifiants « GID » identiques.

8. Une équipe d'une unité chirurgicale peut être composée de : deux chirurgiens, un anesthésiste, un interne, deux infirmières et une secrétaire médicale.

précaution utile afin de garantir la sécurité des informations et notamment d'empêcher qu'elles soient déformées, endommagées ou communiquées à des tiers non autorisés. D'où la nécessité de désigner, pour chaque équipe, un responsable qui a comme tâches supplémentaires : créer l'équipe ; déterminer les habilitations de chaque catégorie de personnel de son équipe ; gérer les transferts dynamiques des membres de son équipe ; identifier les règles de son équipe et mettre à jour ses fonctionnalités.
L'équipe, ainsi que le groupe d'objet qui lui est associé, permettent d'établir le lien entre le professionnel soignant (membre de l'équipe) et le patient traité (dont le dossier, par exemple, est un élément du groupe d'objet associé à l'équipe). En réalité, ce lien est établi dans une structure organisationnelle.

3.5 Notion de contexte

Dans notre modèle, en plus des rôles et des groupes d'objets, nous tenons compte du contexte dans lequel la requête d'accès est faite. Nous distinguons différents types du contexte.

Contexte du rôle : précise des valeurs que doivent prendre certaines variables contextuelles avant d'autoriser/interdire/obliger un utilisateur à jouer un rôle donné. Par exemple : le rôle médecin de salle est valide pendant les heures normales de travail tandis que le rôle médecin de garde est valide la nuit. Aux rôles, sont également associées des contraintes telles que : la cardinalité (le nombre maximal d'utilisateurs autorisés à jouer ce rôle) ; l'exclusion mutuelle (par exemple, dans le même établissement, être personnel soignant et comptable ; l'utilisateur ne peut pas jouer simultanément les deux rôles médecin à l'hôpital et médecin travaillant pour une société d'assurance).

Contexte des objets : des attributs contextuels spécifiques aux objets ou aux groupes d'objets. Par exemple : la durée de conservation des données (les données de neurologie doivent être conservées pendant une durée de 70 ans) ; le lieu : les dossiers de spécialités de chacune des unités sont situés et gérés localement dans les ordinateurs de cette unité.

Attributs des utilisateurs : décrivent des caractéristiques du genre : autorisations spécifiques, droits temporaires, etc. Par exemple : l'affiliation à un corps de santé régional, national ou international ; l'expérience dans la pratique de certains types de soins ; des connaissances spécifiques.

Contexte de l'utilisation : ce concept aide à réaliser un bon compromis entre le respect du *principe du moindre privilège*[9] et la *flexibilité*[10] du contrôle d'accès, dans l'intérêt des patients et le respecter de la législation nationale (CNIL, 1994 ; Décret, 1995) et des directives européennes (Parlement Européen, 1995). Conformément à ces textes, notre vision est d'inscrire toute action dans l'un de ces deux cas :

- 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 (activité en cours) ;
- soit en déclarant un *objectif précis de l'utilisation*. Les règles de sécurité doivent spécifier quel utilisateur/rôle a le droit de déclarer quel objectif, et dans quelles conditions (tout utilisateur n'a pas le droit de déclarer n'importe quel objectif). La finalité doit être clairement définie par le demandeur : situation d'urgence, vérification par un médecin expert auprès d'un tribunal, etc.

Il est évident que les privilèges liés à une utilisation en urgence diffèrent de ceux d'une utilisation à finalité de recherche ou statistique. Certaines utilisations nécessitent le consentement du patient ; d'autres, parfois plus urgentes, tiennent compte de l'objectif mentionné et accordent l'accès avec une responsabilité et une auditabilité plus élevée. Par exemple : afin de favoriser la flexibilité, on peut éditer

9. Ce principe consiste à ne donner accès qu'aux utilisateurs autorisés et seulement pour les ressources dont ils ont besoin pour accomplir leurs tâches

10. La flexibilité consiste ici à ne pas imposer, à cause de la sécurité, des contraintes nuisant au bon fonctionnement du système, donc aux soins du patient.

une règle qui autorise 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 ». Cet objectif sera le point essentiel de l'autorisation et déclenchera automatiquement un audit de haut niveau ou même l'envoi automatique d'une notification au patient. Un autre exemple est d'autoriser, en cas d'urgence, à certains rôles de déclarer l'objectif « traitement d'urgence » et s'accorder des privilèges en assumant leur responsabilité. L'accès sera validé par des valeurs que prendront certaines variables (service des urgences ; patient touché dans un organe vital ; manque de personnel). Pour résumer, le but de « l'objectif de l'utilisation » est d'assurer la flexibilité tout en déterminant la responsabilité de l'utilisateur et d'obtenir une preuve en cas d'abus de pouvoir ou de conflit.

4 Raisonnements à mener sur une politique de sécurité santé/social

A l'inverse d'autres domaines d'applications, les politiques des SICSS doivent permettre d'assurer *simultanément* les propriétés de confidentialité, d'intégrité, de disponibilité et d'auditabilité, dans un univers dynamique où les droits des utilisateurs doivent pouvoir varier selon le contexte courant. Un outil d'assistance à la définition de politiques de sécurité doit donc offrir des mécanismes de raisonnement ou de calcul capables de fournir les services suivants à l'utilisateur.

4.1 Consultation de la politique de sécurité

Une politique de sécurité peut faire l'objet de plusieurs types de requêtes, par exemple :

- quels sont, pour un utilisateur ayant une certaine fonction, les privilèges (permission, interdiction ou obligation) en matière d'action sur un(des) objet(s) donné(s), ou de délégation de privilèges à une autre personne jouant une autre fonction, étant données certaines caractéristiques contextuelles ?
- qui a des privilèges (et lesquels) sur un(des) objet(s) donné(s), et dans quel contexte ?
- dans quel contexte tel utilisateur a tel privilège sur tel objet ou quelle délégation de privilèges ?
- qui peut déléguer quel privilège à un individu remplissant une fonction donnée, dans un contexte donné ou dans quel contexte ? etc. .

4.2 Garantie de certaines propriétés par une politique de sécurité

Il s'agit d'abord de vérifier qu'une politique de sécurité permet de garantir certaines propriétés attendues. Le cas échéant, il faut pouvoir aider son concepteur à la corriger, en localisant si possible les éléments de la politique qui empêchent la garantie de la ou des propriétés souhaitées.

Cohérence d'une politique de sécurité Lorsqu'une politique de sécurité contient des permissions mais aussi des interdictions, voire des obligations, il est nécessaire de s'assurer qu'elle ne peut pas générer de conflit, à savoir que :

- il n'existe pas de situation dans laquelle un utilisateur aurait simultanément la permission et l'interdiction d'effectuer une action sur un objet,
- ni de situation dans laquelle un utilisateur aurait simultanément l'obligation et l'interdiction d'effectuer une action sur un objet.

Le cas échéant, il est souhaitable d'identifier les éléments de la politique (règles) à l'origine de tels conflits, soit les sous-ensembles minimaux de règles générant un conflit dans certaines situations.

Propriétés de sécurité attendues pour une politique de sécurité Il est nécessaire de s'assurer qu'avec une politique de sécurité définie et cohérente, il n'existe pas de situation dans laquelle un utilisateur pourrait violer une propriété de sécurité exigée, par exemple :

- un utilisateur pourrait apprendre une information alors qu'il n'a pas l'autorisation (confidentialité),
- il pourrait créer, modifier ou détruire une information alors qu'il n'en a pas l'autorisation (intégrité).

Il peut être intéressant d'identifier les éléments de la politique provoquant le non respect des propriétés de sécurité souhaitées : les sous-ensembles minimaux de règles qui génèrent l'incohérence dans certaines situations.

4.3 Quelques autres problèmes

L'objectif d'une politique de sécurité est de définir les règles à respecter pour protéger le système contre les menaces et vulnérabilités identifiées lors de l'analyse de risques. Le problème de la complétude d'une politique de sécurité peut être vu comme celui de l'exhaustivité du règlement correspondant. Ceci peut être vérifié en montrant que, face à chaque risque identifié, il existe une règle spécifiée dans la politique de sécurité qui définit la conduite à tenir face à ce risque. Des problèmes de fusion de politiques de sécurité peuvent également se poser, par exemple dans le cadre d'une restructuration entre deux organismes. Un premier aspect concerne la définition de rôles et de structures organisationnelles qui soient compatibles. Un autre aspect concerne ensuite la détection de conflits dans la politique obtenue par fusion, puis la proposition d'une méthode permettant de résoudre ces conflits. Des problèmes analogues se posent si l'on souhaite faire interopérer deux organisations dotées chacune de sa propre politique de sécurité.

5 Types d'approches formelles envisagées

Un des objectifs de MP6 est d'offrir des outils formels pour vérifier qu'une politique de sécurité respecte les propriétés attendues. Nous utiliserons la capacité expressive et le mécanisme déductif des logiques non classiques pour exprimer formellement les politiques de sécurité et pour vérifier automatiquement si ces politiques sont correctes vis-à-vis de telle ou telle propriété de sécurité. L'utilisation des logiques non classiques est nécessaire pour la prise en compte de concepts déontiques comme l'obligation ou l'interdiction, mais aussi pour la gestion des conflits qui peuvent apparaître au sein d'une politique de sécurité. Pour aborder ces problèmes, deux familles de logiques non classiques sont considérées : la logique modale et la logique possibiliste.

La logique modale est une extension de la logique classique dans laquelle, en plus des connecteurs booléens comme la disjonction ( ), la conjonction ( ) ou la négation (¬), on trouve les connecteurs intensionnels et . La logique modale est appelée logique déontique lorsque les formules A et A sont lues « il est obligatoire que A » et « il est permis que A » respectivement. Le concept d'interdiction n'est pas oublié puisque la formule ¬A exprime justement l'interdiction de A. Des exemples particulièrement intéressants de formules déontiques utiles pour représenter les politiques de sécurité sont les formules de la forme C_1 C_n A (« si les conditions C_1, , C_n sont vérifiées alors A est obligatoire ») ou C_1 C_n A (« si les conditions C_1, , C_n sont vérifiées alors A est permis »). La lecture déontique de la logique modale soulève des questions théoriques mais aussi pratiques. Il y a d'abord la question de l'interprétation sémantique des formules du langage de la logique déontique. Cette interprétation sémantique est réalisée dans des structures relationnelles appelées « modèles de Kripke » au sens habituel de la logique modale (Hughes et Cresswell, 1984). Il y a ensuite la question

de la mécanisation du raisonnement dans ces structures relationnelles, c'est-à-dire, étant donnée une formule, montrer qu'il existe une structure relationnelle qui la satisfait. A cet égard des techniques de déduction automatique, basée par exemple sur la méthode des tableaux (Fitting, 1983), ont été proposées. La mécanisation du raisonnement en logique déontique permet d'automatiser le test de la cohérence des politiques de sécurité. La gestion des conflits détectés au moyen de cette technique est réalisée par la logique possibiliste.

La logique possibiliste est aussi une extension de la logique classique. L'idée est d'associer à chaque formule un degré qui reflète son niveau de priorité. Les notions de cohérence et inférence de la logique classique deviennent graduelles, donnant respectivement les mesures de possibilité et nécessité.

L'un des avantages de la logique possibiliste est sa capacité à traiter des informations conflictuelles. Considérons deux règles : "(i) le personnel non médical n'est pas autorisé à lire les dossiers médicaux des patients", et (ii) "un patient peut lire son dossier médical, même s'il ne fait pas partie du personnel médical". En logique classique, ces deux règles sont conflictuelles dès qu'un patient demande l'autorisation de lire son dossier médical. La logique possibiliste, grâce à un algorithme de stratification développée dans (Benferhat *et al*., 1998), associe automatiquement une priorité plus élevée à la règle (ii), et de ce fait en présence de conflits seule la deuxième règle est appliquée (Benferhat *et al*., 2002).

Les propriétés de confidentialité et d'intégrité peuvent être facilement exprimées en logique possibiliste. Ainsi, la confidentialité est vérifiée au moyen d'un test de cohérence entre la base de connaissances et une contrainte de la forme "si un utilisateur lit un document, alors il a la permission de le lire".

6 Conclusion

Les SICSS sont des systèmes complexes, riches en fonctionnalités, qui deviennent de plus en plus exigeants en matière de sécurité. Il est donc indispensable de définir au préalable une politique de sécurité qui soit à la fois robuste, efficace, flexible, assez générique et pour laquelle la vérification des propriétés de sécurité soit possible.

Dans cette optique, le travail que nous avons présenté commence par une description des SICSS et de leurs environnements, de leurs vulnérabilités et des menaces potentielles. Pour faire face aux risques identifiés, les objectifs de sécurité s'expriment en terme de disponibilité, de confidentialité, d'intégrité et de responsabilité. L'article montre que les modèles de politiques existants dans l'état de l'art actuel sont incapables de couvrir les spécificités des SICSS; en effet, soit ils sont très rigides et visent à satisfaire une seule propriété, soit ils sont mal employés et ne résolvent pas tous les problèmes. Nous avons donc défini de nouveaux concepts (rôle, équipe, groupe d'objet et contexte) et méthodes pour appréhender l'ensemble des besoins soulevés. Nous avons également présenté les principaux types de vérifications souhaitables sur une politique de sécurité; enfin nous avons proposé des langages formels permettant à la fois de représenter une politique, et de mener automatiquement les calculs pour s'assurer qu'elle vérifie bien des propriétés souhaitables; ces approches sont basées essentiellement sur l'utilisation des logiques déontique et possibiliste.

Nous envisageons maintenant d'enrichir notre politique pour satisfaire des besoins élevés en terme de propriétés de sécurité et vérifier la cohérence d'une politique de sécurité. La suite des travaux consistera à préparer un processus d'évaluation et pour cela proposer un gabarit de sécurité à mettre en œuvre et à définir des mécanismes à implémenter, pour permettre d'atteindre des objectifs de sécurité exigeants et, ainsi, pouvoir protéger les SICSS contre les diverses menaces identifiées.

7 Références

Abou el Kalam, A. (2002). “Politiques de sécurité pour les systèmes d'informations médicales”, *Journées Doctorales en Informatique et Réseaux (JDIR)*. Toulouse, France, pp. 201-210.

Abou El Kalam, A. et Y. Deswarte (2002). “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”. *Actes de la conférence Sécurité et Architecture des Réseaux (SAR’02)*, p.11.

BCN 84 (1998). “Droits d’accès au dossier, Dossier Médical Global informatisé”, *Bulletin du Conseil National du 12 décembre 1998*. BCN n° 84, juin 1999 , p.14.

Bell, D.E. et L.J LaPadula (1975). “Secure Computer Systems : Unified Exposition and Multics Interpretation”. *The MITRE Corporation, Technical Report, ESD-TR-73-306*.

Benferhat, S., D. Dubois et H. Prade (1998). “Practical Handling of Exception-Teinted Rules and Independence Information in Possibilistic Logic”. *Applied Intelligence*, 9, pp.101-127

Benferhat, S., R. El Baida et F. Cuppens (2002). “Modélisation des politiques de sécurité dans le cadre de la théorie des possibilités”. *Rencontres francophones sur la logique floue et ses applications*. Montpellier, 21-22 Octobre 2002.

Chellas, B.F.(1980). “Modal Logic : An Introduction”. *Cambridge University Press*. ISBN 0-521-29515-7.

CNIL (1994). *Rapports d’activité de la CNIL n° 15*.

Conseil de l’Europe (1981). Recommandations du Conseil de l’Europe, R(81) 1, “*On Automated Medical Data Banks*”, article 29, Council of Europe, Strasbourg.

Decret (1995). Décret 95-1000 du 6 septembre 1995 portant sur le code de déontologie médicale.

Fitting, M. (1983). “*Proof Methods for Modal and Intuitionistic Logics*”. D. Reidel Publishing Company.

Gavrila, S.I. et J.F. Barkley (1998). “Formal Specification for Role Based Access Control”. *Third ACM Workshop on Role-Based Access Control*. Fairfax, VA, USA.

Hughes, G.E. et M.K. Cresswell (1984). *A Companion to Modal Logic*. Methuen

Loi (1991). Loi n° 91-748 du 31 juillet 1991 portant réforme hospitalière et décret n° 92-329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés.

Parlement Européen (1995). Directive 95/46/CE du parlement Européen, adoptée par le Conseil Européen 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*.

Sandhu, R., E.J. Coyne, H.L. Feinstein et C.E. Youman (1996). “Role-Based Access Control Models”, *IEEE Computer*, vol.29, pp.38-47.

Trouessin, G. (2001). “Sécurité et intimité des données à caractère personnel”. *La Lettre d’ADELI n°42*, juillet 2001.

Trouessin, G. (2002). “L’évolution des normes de sécurité vers plus d’auditabilité des systèmes d’information”. *Colloque AIM à l’HEGP : «Présent et avenir des systèmes d’information et de communication hospitaliers»*, 23-24 mai 2002 (à paraître chez Springer-Verlag).