Politiques formelles d'échange d'informations critiques dans les organisations

Claire Saurel

ONERA Toulouse, France
claire.saurel@onera.fr

RÉSUMÉ. *Cet article propose une extension d'un outil formel permettant de définir et analyser des politiques d'échange d'informations entre agents au sein d'organisations utilisatrices d'un système d'informations critiques. Ces règles d'échange d'informations sont avant tout définies pour des besoins liés au métier, selon les rôles tenus par les agents dans les organisations ; elles dépendent de la structure de l'organisation. Nous définissons donc un niveau de langage pour exprimer des politiques à un niveau plus abstrait que celui des individus : celui des organisations. Des propriétés génériques ou spécifiques souhaitables pour une politique peuvent être définies à ce même niveau, en particulier la propriété de perméabilité d'information. Le gain attendu avec cette extension concerne une plus grande efficacité d'expression, d'analyse et de mise à jour des politiques d'échange.*

ABSTRACT. *This paper starts from a logical framework intended to define and analyse information exchange policies for users of critical information systems within some organisations. These information exchange rules are defined according to the roles users play in organisations: so they depend on the structure of organisations. A layer is then introduced to express organisational information exchange policies at a more abstract level than users level: organisational level. Generic and specific properties can be defined within this organisational layer, in particular information permeability through organisations. More efficiency is expected for policies expression, analysis and update.*

MOTS-CLÉS : *politiques d'échange d'informations, sécurité des informations, organisation, rôle, héritage, modélisation formelle, analyse formelle, information critique.*

KEYWORDS: *information exchange policy, information security, organisation, role, rights inheritance, formal modelling, formal analysis, critical information.*

DOI:10.3166/ISI.21.4.27-47 © 2016 Lavoisier

1. Introduction

Dans les systèmes d'informations critiques, comme les systèmes de surveillance de débris spatiaux [1], les systèmes de gestion de crise humanitaire ou terroriste, les systèmes de veille sanitaire etc., il est impératif de permettre aux utilisateurs de diverses organisations d'échanger de l'information sensible de manière à pouvoir en dériver des conclusions pertinentes et d'intérêt commun, tout en préservant la confidentialité de ces informations. Par exemple (Mandl *et al.*, 2004 ; Parks, 2004), un système de veille sanitaire peut faire collaborer des personnels de laboratoires d'analyse de sang ou d'analyse épidémiologique, des cabinets médicaux et des hôpitaux dont les médecins voient des patients, des écoles dont les directeurs constatent des absences d'élèves, des pharmacies qui doivent répondre à des demandes accrues de certains médicaments, tous situés dans une zone géographique commune, pour permettre, à partir d'informations privées recueillies sur des individus, la détection au plus tôt de certaines épidémies d'origine virale ou bioterroriste.

Il est également crucial d'éviter la diffusion d'informations dénuées d'intérêt à certains utilisateurs, de manière à garantir l'efficacité des échanges et du système. Enfin, il est primordial que des utilisateurs dotés de pouvoirs de décision reçoivent sans faute et en temps opportun les informations nécessaires à la réalisation de leur travail de manière la plus efficace possible.

On cherche à gagner la confiance des personnels impliqués dans de tels systèmes, condition absolue pour un partage d'informations essentiel à la réussite de la mission du système. Pour contrôler et protéger les échanges d'informations critiques ou sensibles, une démarche classique en sécurité informatique consiste à autoriser seulement les accès souhaitables à certaines informations ou opérations [2]. Mais ici, nous voulons aussi pouvoir garantir par exemple que les informations nécessaires au travail de certains utilisateurs leur seront envoyées systématiquement, à bon escient, ou en temps utile [3]. C'est pourquoi il est donc préférable, dès la phase de spécification et en amont du développement du système, d'en définir d'abord une politique globale d'échange d'informations comme exigence à satisfaire par le futur système, et sur laquelle les différents partenaires utilisateurs du système soient d'accord : il s'agit ici d'une réglementation, autrement dit d'un ensemble de règles explicitant sous quelles conditions il est obligatoire, permis ou interdit à un utilisateur d'envoyer une information, ou un type d'information, à d'autres utilisateurs.

Il est interdit aux officiers de sécurité d'envoyer une information sur une attaque à l'anthrax à des journalistes est un exemple d'une telle règle.

En réalité, les politiques d'échange d'informations ne sont généralement pas pensées et définies explicitement pour les entités individuelles appartenant à une orga-

1. Spatial Awareness Systems.
2. Par exemple, avec des moyens de chiffrement, ou des contrôles d'accès.
3. Ce qui se traduit en terme d'*obligation* d'envoyer l'information aux destinataires concernés.

nisation - qu'elle soit virtuelle ou réelle, ou pour chacune des informations qu'elles sont amenées à s'échanger. Elles visent plutôt à réglementer et contrôler les échanges d'informations critiques entre utilisateurs pour des besoins liés à leur métier, en fonction des différents rôles qu'ils occupent dans l'organisation dans laquelle ils doivent collaborer. Nous définissons une politique d'échange d'informations comme un ensemble de règles régissant les droits (au sens large [4]) de classes d'utilisateurs vis-à-vis d'autres classes d'utilisateurs, concernant des catégories d'informations qu'ils peuvent être amenés à traiter dans le cadre de leur fonction.

Selon les organisations, les devoirs attachés à un rôle peuvent différer. Dans le cas d'un système de veille sanitaire, le secrétaire d'un médecin privé doit envoyer des résultats d'analyse de sang au secrétaire du laboratoire d'analyse épidémiologique, alors que ce dernier doit envoyer les conclusions d'épidémies décelées au ministère de la Santé. Les échanges d'informations doivent aussi parfois vérifier des propriétés souhaitées par les organisations : dans le cas précédent, les résultats transmis ne doivent pas permettre de dévoiler l'identité d'un patient concerné; en revanche ils doivent être retournés au plus vite aux médecins des malades pour permettre le début de soins, ou aux autorités pertinentes qui doivent décider au plus tôt des mesures de protection ou prévention qui s'imposent. Toutes ces contraintes concernent les envois d'informations à effectuer selon les rôles concernés dans les organisations impliquées dans le système d'informations, indépendamment des personnes qui jouent ces rôles.

De manière générale, une organisation souhaite définir des règles d'échange concernant :

– des catégories d'informations présentant de l'intérêt pour son métier - et seulement celles-là,

– des rôles définis par l'organisation, les rôles étant joués par des agents (individus) amenés à changer au fil du temps,

– des conditions données, propres à l'organisation,

qui doivent permettre de garantir des propriétés souhaitées.

La notion de rôle et sa différenciation par rapport au concept d'agent ont été introduites depuis longtemps dans de nombreuses communautés scientifiques, comme en logique multi-agents (Pacheco, Carmo, 2003) avec la notion d'agent institutionnel (Carmo, Pacheco, 2001), ou en sécurité informatique pour définir dans des organisations des contrôles d'accès en termes de permissions (Sandhu *et al.*, 1996).

D'un point de vue conceptuel, la notion de rôle dans une organisation va bien au-delà de la simple représentation de l'ensemble des agents qui le jouent à un instant donné. Un rôle correspond à une fonction à remplir dans l'organisation ; il fait partie de la description de la structure d'une organisation ou d'une entreprise, indépendamment des agents (personnes ou logiciels) amenés ponctuellement à remplir ce rôle. Dans

4. Obligation, permission ou interdiction d'échanger, c'est-à-dire d'envoyer de l'information à quelqu'un.

la littérature sur la modélisation des organisations, un rôle est souvent caractérisé par l'ensemble des responsabilités d'activités ou de tâches confiées aux acteurs ou agents affectés au rôle par l'organisation (Glassey, Chappelet, 2002), des ressources, et des obligations, permissions ou interdictions associées à ces tâches. Afin d'éviter des effets ou abus non souhaitables concernant les acteurs de rôles, sont également souvent rattachées aux définitions de rôles des contraintes d'exclusion mutuelle ou de dépendances avec d'autres rôles, qui s'appliquent dans le processus d'affectation d'agents aux rôles (Pacheco, Carmo, 2003) : par exemple, les contraintes dites de séparation de pouvoir permettent d'éviter des conflits d'intérêt pour un agent qui pourrait jouer plusieurs rôles.

Par ailleurs, il est important de pouvoir localiser et délimiter facilement la partie de la politique qui sera impactée par une mise à jour (Benferhat *et al*., 2003 ; Kalam *et al*., 2003). Or dans une organisation, la structure de l'organisation évolue généralement plus lentement que les agents qui y jouent un rôle. En cas de changement d'employés dans l'organisation, ou de modification des affectations des employés à un rôle, le fait d'avoir défini et formulé une politique d'échange des informations directement en termes des rôles structurant l'organisation évite ainsi d'avoir à la modifier aussi souvent que si elle ciblait directement les employés.

Il est donc souhaitable d'identifier et structurer de manière adéquate un ensemble des concepts primitifs facilitant la définition et la description d'une politique d'échange d'informations pour une organisation, de manière à faciliter aussi ses analyses, et à rendre moins coûteuses ses mises à jour les plus fréquentes. Nous proposons d'articuler cet ensemble autour des notions de rôle et d'organisation.

Pour permettre de formuler de manière satisfaisante et convaincante une politique d'échange d'informations, une approche formelle présente un double intérêt :

– elle oblige les utilisateurs à exprimer clairement et sans ambiguïté la réglementation souhaitée dans un langage rigoureux, limitant ainsi les possibilités d'interprétations multiples,

– et elle propose des outils de calcul automatique pour vérifier des propriétés requises par les utilisateurs, sur leur politique exprimée dans le langage formel choisi.

L'outil formel PEPS (Delmas, Polacsek, 2013) a été conçu pour aider des utilisateurs [5] à concevoir et analyser des politiques d'échange d'informations répondant à des exigences re-quises par les utilisateurs. Cet outil propose un langage logique du premier ordre multisorte [6] (Rozière, 2004) basé sur les concepts primitifs d'information et d'agent. PEPS intègre également des modalités déontiques (cf section 2) associées et intégrées à une action *envoyer*. Il est possible d'utiliser PEPS pour définir une politique comme un jeu de règles stipulant sous quelles conditions des *agents*

5. Dans la suite de cet article, nous utilisons le terme utilisateur pour une personne en charge de définir une politique d'échange.

6. ie, permettant de manipuler plusieurs types d'objets.

ont l'obligation, la permission ou l'interdiction d'envoyer des informations à d'autres *agents*, puis d'analyser la politique et de la modifier jusqu'à ce qu'elle remplisse des propriétés souhaitées.

PEPS s'avère être un outil interactif puissant et relativement convivial. Notre objectif est donc de l'enrichir avec une couche organisationelle définie au-dessus du langage existant ; le but est de permettre aux utilisateurs d'exprimer et analyser une politique d'échange formulée directement au niveau organisationnel, dans un souci de lisibilité et de clarté, tout en profitant de l'efficacité de PEPS.

Dans cet article, la section 2 décrit l'environnement initial PEPS d'un point de vue théorique et pratique. La section 3 introduit une couche dans le langage PEPS pour permettre d'exprimer des politiques d'échange au niveau des organisations. La section 4 propose des jeux d'axiomes de transmission de droits d'échange d'informations entre rôles et organisations. La section 5 définit quelques propriétés générales et plus spécifiques pour des politiques, dans le contexte des organisations. La dernière section conclut l'article.

2. PEPS : un environnement logique pour exprimer des politiques d'échange d'informations orientées agents

PEPS (Delmas, Polacsek, 2013) est un environnement formel avec deux composantes : un langage logique du premier ordre multisorte pour exprimer des politiques d'échange d'informations entre agents, et un solver SAT pour vérifier des propriétés définies dans ce même langage sur l'expression formelle des politiques. Les principaux concepts primitifs proposés dans PEPS sont l'information, l'agent, et les trois modalités déontiques d'obligation, permission, et interdiction directement et exclusivement associées à l'action envoyer, seule action réglementée dans une politique d'échange. Étant donnée une politique définie avec ce langage, PEPS propose un analyseur pour vérifier des propriétés prédéfinies comme la consistance [7], l'applicabilité [8], la minimalité [9] ou la complétude [10]; il peut aussi vérifier des propriétés spécifiques métier, dans la mesure où elles sont décrites par l'utilisateur dans PEPS.

Le langage PEPS est défini par un quadruplet $\{Sort, Var, Fun, \sigma\}$, dont les composantes dénotent respectivement les ensembles des identificateurs de sortes, de variables, de fonctions, ainsi que les signatures des fonctions. Les prédicats sont des fonctions dont le résultat est de type booléen. Les constantes sont des fonctions sans argument.

---

7. Dans certaines situations, une politique inconsistante pourrait mettre un agent face au dilemme d'avoir à la fois la permission et l'interdiction d'envoyer une information à un autre agent.

8. La politique ne réglemente pas de situation ne pouvant jamais se produire.

9. La politique ne contient pas de règle déductible à partir d'autres qu'elle contient déjà.

10. Dans tous les cas, la politique spécifie aux agents s'ils ont l'obligation, la permission ou l'interdiction d'envoyer une information à un autre agent.

Les sortes prédéfinies dans PEPS comprennent : $\mathcal{A}$ (agents), $\mathcal{I}$ (informations), et $\mathcal{T}$ (topics, ou thèmes).

Les prédicats et les constantes sont donc des fonctions particulières. Parmi les prédicats prédéfinis figurent : $K(a, i)$ (l'agent a connaît l'information i) et $Topic(i, t)$ (l'information i concerne le thème t).

La logique déontique [11] (von Wright, 1951 ; Chellas, 1980) est une logique modale dont les modalités [12] traduisent des concepts déontiques s'appliquant de manière générique à des prédicats. Pour exprimer des normes, i.e. des règles spécifiant ce qu'il est obligatoire, permis ou interdit de faire [13], il est pratique d'utiliser des modalités déontiques. Pour modéliser et raisonner avec ces concepts déontiques, il semblait toutefois plus simple de réutiliser des outils efficaces en logique du premier ordre, plutôt que d'utiliser une logique modale : les auteurs de $peps$ ont donc choisi de rester dans le cadre d'une logique du premier ordre, en proposant des prédicats normatifs définis en associant directement les modalités déontiques à la seule action *envoyer* : $O_{Send}(a, b, i)$ (respectivement : $F_{Send}(a, b, i)$, $P_{Send}(a, b, i)$) signifie que l'agent a a l'obligation (respectivement : l'interdiction, la permission) d'envoyer l'information i à l'agent b.

De manière classique comme en logique déontique (Chellas, 1980), un axiome relie l'obligation d'envoyer et la permission d'envoyer : toute obligation d'envoyer une information donne lieu à la permission de l'envoyer.

Par exemple, supposons que la règle suivante ait été définie pour une équipe en charge d'attaques à l'anthrax, au sujet de la diffusion d'informations sur le thème $Anthrax$:

"Tout agent a qui connaît i se rapportant au thème $Anthrax$ a l'obligation d'envoyer i à l'agent $Martin$".

Dans PEPS , les symboles de prédicats et de constantes commencent par des majuscules, à l'inverse des symboles de variables. Ainsi, une formulation de la règle ci-dessus en PEPS peut être :

$$\forall a, \forall i,\ Topic(i, Anthrax) \wedge K(a, i) \implies O_{Send}(a, Martin, i)\ .$$

A noter que l'utilisateur a la possibilité d'étendre le langage natif de PEPS en définissant ses propres sortes, fonctions et prédicats, pour élargir l'ensemble des concepts de base initialement proposés.

---

11. La notion de déontique se rapporte à la formulation de règles morales.

12. Une modalité modifie un énoncé en le qualifiant, selon la modalité, de : nécessaire, obligatoire, vrai dans le futur, etc. Une modalité déontique attache donc une indication de valeur morale à un énoncé : elle exprime le devoir en terme d'obligation, permission ou interdiction attachée à un état, comme par exemple : "Il est obligatoire pour une secrétaire d'envoyer telle information à son directeur".

13. Ici, les normes requises ne concernent que l'envoi d'informations.

L'interface de l'outil PEPS permet à l'utilisateur de définir une politique d'échange d'informations entre agents comme un ensemble de règles de la forme ci-dessus, ainsi que de décrire les lois et connaissances d'un domaine d'application. Un éditeur lui permet de formuler des propriétés spécifiques à vérifier sur une politique plongée dans un contexte applicatif décrit. Le module Analyseur de PEPS, basé sur un solveur SAT, permet à l'utilisateur de vérifier interactivement si, étant donné un contexte applicatif, une politique garantit des propriétés générales prédéfinies comme : consistance, complétude (Cholvy *et al.*, 2006 ; 2007), minimalité, et applicabilité (Delmas, Polacsek, 2013), ou des propriétés plus spécifiques à son application, exprimées dans le langage de PEPS. Dans le cas d'une propriété non vérifiée par la politique, l'analyseur retourne à l'utilisateur un modèle prouvant la non satisfaisabilité : l'utilisateur dispose ainsi d'indications pour modifier sa politique, tester à nouveau si une propriété requise est vérifiée, etc. jusqu'à obtenir une politique qui lui convienne.

3. PEPS-ORG : une couche au-dessus de PEPS pour exprimer et analyser des politiques organisationnelles d'échange

Pour permettre d'exprimer dans l'environnement PEPS des règles d'échange d'informations au sein d'organisations, nous définissons des sortes pour exprimer quelques concepts primitifs : $\mathcal{O}$ et $\mathcal{R}$ dénotent respectivement les organisations et les rôles.

Comme dans (Benferhat *et al.*, 2003), nous introduisons le prédicat $Enpower$, où $Enpower(org, a, r)$ signifie qu'une organisation org affecte un agent a au rôle r. Notons que, comme dans (Benferhat *et al.*, 2003), un agent peut être affecté à plusieurs rôles, dans une ou plusieurs organisations. Pour une application donnée, un ensemble de formules PEPS comprenant ce prédicat $Enpower$ décrira une partie de la connaissance sur une organisation.

Pour définir une politique d'échange, nous avons besoin d'exprimer deux classes d'informations supplémentaires : les contraintes du domaine applicatif sur des rôles dans les organisations, puis les règles d'échange d'informations entre les rôles.

3.1. Contraintes sur les rôles

Nous souhaitons pouvoir formuler des contraintes sur les rôles et les organisations pour préciser le nombre d'agents individuels pouvant jouer un rôle donné, ou pour spécifier les cas où plusieurs rôles peuvent être attribués à un même agent. Pour cela, nous introduisons a minima les deux prédicats suivants dans PEPS-ORG :

– $Exclusive(r, o)$ signifie [14] que dans l'organisation o, le rôle r ne peut être affecté qu'à un seul agent.

14. $Exclusive(r, o) \equiv \forall a, b, \quad Enpower(o, r, a) \wedge Enpower(o, r, b) \implies \neg Distinct(a, b)$

– $Incompatible(r, o, r', o')$ signifie [15] qu'aucun agent ne peut jouer à la fois les rôles r dans o, et r' dans o'. Bien sûr, nous posons : $\neg Incompatible(r, o, r, o)$.

Ainsi, la contrainte *"Personne ne peut jouer le rôle de $SecurityOfficer$ à la fois dans l'organisation O et dans une autre organisation"* se formule par :

$\forall o,$

$$Distinct^{org}(o, O) \implies Incompatible(SecurityOfficer, O, SecurityOfficer, o)$$

Pour une application et des organisations données, Σ^{org} dénote l'ensemble des formules exprimant des contraintes sur les rôles.

3.2. Politiques organisationnelles d'échange d'informations

PEPS ne propose pas le mécanisme d'héritage entre sortes : il n'est donc pas possible d'utiliser au niveau organisationnel ses prédicats normatifs O_{Send}, P_{Send} et F_{Send}, dont des termes sont de type agent individuel et non pas rôle. L'introduction nécessaire de prédicats dédiés pour traiter des rôles au niveau organisationnel offre néanmoins l'avantage de donner une meilleure lisibilité aux formules décrites dans le langage.

$O^{org}_{Send}(r, o, r', o', i)$, $P^{org}_{Send}(r, o, r', o', i)$ et $F^{org}_{Send}(r, o, r', o', i)$ dénotent respectivement l'obligation, la permission et l'interdiction pour un rôle r dans une organisation o (c'est-à dire, aux agents affectés au rôle r) d'envoyer une information i à un rôle r' dans une organisation o' (ie, aux agents affectés au rôle r').

Quoique cela alourdisse un peu le langage, nous choisissons de spécifier les organisations auxquelles appartiennent les rôles r et r' car nous ne faisons pas l'hypothèse d'unicité des identifiants de rôle : ainsi, les droits [16] définis pour un secrétaire peuvent varier d'une organisation à l'autre; par ailleurs, il nous semble légitime de permettre à une organisation de préciser les organisations auxquelles elle souhaite qu'une information soit envoyée ou pas.

Comme en logique déontique (Chellas, 1980), pour assurer une sorte de cohérence entre les notions d'obligation et de permission, nous introduisons l'axiome suivant qui indique que tout rôle ayant l'obligation d'envoyer une information à un rôle doit aussi en avoir la permission :

$$(D^{org}) \quad \forall r1\ , \forall r2\ , \forall o1\ , \forall o2\ , \forall i,$$
$$O^{org}_{Send}(r1, o1, r2, o2, i) \implies P^{org}_{Send}(r1, o1, r2, o2, i)$$

---

15. $Incompatible(r, o, r', o') \equiv \forall a, b,$
$(Distinct^{org}(o, o') \vee Distinct^{role}(r, r')) \wedge (Enpower(o, r, a) \wedge Enpower(o', r', b) \implies Distinct(a, b))$ où $Distinct^{role}$, $Distinct^{org}$ et $Distinct$ sont des prédicats prédéfinis, traduisant respectivement que deux rôles (respectivement : deux organisations, deux agents) ne sont pas identiques.

16. i.e. obligations, permissions ou interdictions pour les rôles d'envoyer des informations à d'autres rôles.

En reprenant la démarche de (Delmas, Polacsek, 2013), une règle organisationnelle d'échange est définie par :

DEFINITION 1 (Règle organisationnelle d'échange d'informations). — .

Une règle organisationnelle d'échange est une formule fermée de PEPS *d'une des trois catégories suivantes :*

$$Qx_1, \ldots, Qx_n,\ (\phi \implies O^{org}_{Send}(r_1, o_1, r_2, o_2, i))$$
$$Qx_1, \ldots, Qx_n,\ (\phi \implies P^{org}_{Send}(r_1, o_1, r_2, o_2, i))$$
$$Qx_1, \ldots, Qx_n,\ (\phi \implies F^{org}_{Send}(r_1, o_1, r_2, o_2, i))$$

où :

– *Q est un quantificateur logique $\forall$ ou $\exists$;*

– *$x_1, \ldots, x_n$ sont toutes des variables de ϕ, r_1, o_1, r_2, o_2, et i ;*

– *ϕ est une formule sans quantificateur ni prédicat normatif défini pour le niveau organisationnel;*

– *r_1, r_2 sont des termes de la sorte $\mathcal{R}$, o_1, o_2 sont des termes de la sorte $\mathcal{O}$; i est un terme de la sorte $\mathcal{I}$.*

Supposons que O et OJ soient deux organisations employant respectivement des officiers de sécurité et des journalistes, voici un exemple d'une telle règle :

$$\forall i : \mathcal{I},\ Topic(i, Anthrax) \implies F^{org}_{Send}(SecurityOfficer, O, Journalist, OJ, i).$$

i.e. : dans l'organisation O, il est interdit à un officier de sécurité de transmettre une information concernant le thème $Anthrax$ à un journaliste de l'organisation OJ.

Nous désignons par PEPS-ORG la restriction de PEPS aux formules des sections 3.1 et 3.2, ne concernant que des rôles, des organisations et des informations.

A noter qu'il n'est pas possible dans PEPS-ORG d'exprimer des règles qui réglementent la diffusion d'information entre des rôles et des agents individuels : si l'utilisateur pense avoir besoin de le faire, nous lui suggérons de se demander si ces agents individuels ne sont pas identifiés implicitement au rôle qu'ils jouent, et de réfléchir plutôt en termes de structure d'organisation.

DEFINITION 2 (Politique organisationnelle d'échange d'informations). —

Une politique organisationnelle d'échange d'informations OEP est un ensemble de règles organisationnelles d'échange d'information entre rôles dans des organisations.

DEFINITION 3 (Spécification d'une politique organisationnelle d'échange d'informations). —

Une spécification d'une politique organisationnelle d'échange d'informations est un couple $OEPS = \langle \Sigma, OEP \rangle$, où Σ décrit toutes les lois ou connaissances du domaine d'application [17]*, incluant Σ^{org}* [18]*, et où OEP est une politique organisationnelle d'échange d'informations, Σ^{org} et OEP étant exprimées dans* PEPS-ORG.

3.3. Droits de transmission d'informations entre rôles et agents individuels

Soit une politique organisationnelle d'échange d'informations exprimée à l'aide de PEPS-ORG, il convient de préciser comment se définissent les droits de diffusion des agents individuels à partir de la politique.

AXIOME 4 (Transmission de l'obligation des rôles aux agents). —

$$\forall a, b,\ \ \forall r1, r2,\ \ \forall o1, o2,\ \ \forall i,$$
$$K(a, i) \wedge \mathit{Enpower}(o1, a, r1) \wedge \mathit{Enpower}(o2, b, r2) \wedge O^{org}_{Send}(r1, o1, r2, o2, i)$$
$$\Longrightarrow\ O_{Send}(a, b, i)$$

autrement dit : si, au niveau organisationnel, il y a obligation pour un rôle $r1$ de l'organisation $o1$ d'envoyer une information i au rôle $r2$ dans l'organisation $o2$, alors tout agent a affecté au rôle $r1$ dans $o1$ qui apprend une information i a l'obligation d'envoyer i à tout agent b affecté au rôle $r2$ dans $o2$.

Cet axiome est assez fort, car les agents a et b sont quantifiés universellement : *tous* les agents jouant le rôle $r1$ dans $o1$ ont donc l'obligation d'envoyer i à *tous* les agents jouant le rôle $r2$ dans $o2$; dans certains cas on pourrait souhaiter se contenter par exemple d'exiger l'envoi de i à (seulement) au moins un agent jouant $r2$ dans $o2$. Il est possible de définir des variantes de l'axiome 4 moins contraignantes avec des quantificateurs existentiels (par exemple, au moins pour l'agent b) : par souci de simplification, nous nous limitons ici à cette version.

Nous utilisons des axiomes similaires pour la transmission des rôles aux agents des permissions et des interdictions de diffuser de l'information. Notons que comme concrètement les actions sont effectuées par des agents et non pas par des rôles (Pacheco, Carmo, 2003), le prédicat K qui apparaît dans les règles formulées en PEPS n'apparaît pas dans les règles formulées en PEPS-ORG.

Dans la suite de ce travail, nous envisageons seulement des applications pour lesquelles les axiomes ci-dessus sont pertinents.

---

17. i.e. : contraintes d'intégrité, ontologie des thèmes intéressant les organisations, lois du domaine d'application...

18. Σ^{org} désigne l'ensemble des contraintes exprimées sur les rôles dans les organisations (voir les sections 3.1, puis 4.2).

4. Transmission de droits entre rôles ou organisations

En nous inspirant de (Cuppens *et al*., 2004), nous considérons deux modes de transmission de droits : au sein d'une hiérarchie de rôles et au sein d'une hiérarchie d'organisations.

4.1. Transmission de droits au sein des organisations en sécurité informatique

Les premiers travaux à s'intéresser au principe de transmission des droits (dit aussi : héritage de droits) ont été ceux de la communauté de Sécurité Informatique au sujet des politiques d'accès, dans les années 1990.

Le modèle RBAC (Sandhu *et al*., 1996) a été proposé pour contrôler les droits d'accès à des ressources au sein d'organisations, ces droits étant alors limités à des permissions d'accès. De manière originale, il proposait d'exploiter une hiérarchie entre rôles (par exemple, cet ordre reflétant la responsabilité administrative) pour permettre aux rôles préférés d'hériter des permissions déjà accordées explicitement aux rôles moins préférés. Par exemple, dans le cadre d'une relation d'ordre traduisant une hiérarchie administrative, supposons que le rôle *directeur* soit préféré au rôle *employé* [19]. Avec le principe de transmission de droits proposé dans RBAC, le rôle de directeur hérite de toutes les permissions d'accès accordées au rôle d'employé. Une règle de transmission de droits est une façon élégante de faire l'économie du travail de devoir spécifier explicitement toutes les règles de diffusion s'appliquant à tous les rôles. Son utilisation permet aussi d'exprimer une politique d'échange de manière plus concise.

Hélas, cette astuce est parfois trop radicale et peut donner des résultats non souhaitables, selon la nature de la relation d'ordre considérée entre les rôles (Crampton, 2003 ; Feldmeier, 2006 ; Cuppens *et al*., 2004), et selon la nature du droit considéré : permission, obligation mais aussi interdiction. Par exemple, dans le cas d'un rôle qui est à la fois administrativement supérieur mais techniquement moins qualifié qu'un autre (comme un directeur d'hôpital qui ne serait que médecin, alors que ses employés pourraient être chirurgiens), il n'est pas pertinent que ce rôle hérite des droits des rôles qui lui seraient administrativement inférieurs mais techniquement plus qualifiés : les directeurs pourraient se voir dotés de droits que leurs compétences insuffisantes ne leur permettraient pas d'utiliser à bon escient; de plus, ils pourraient hériter de droits non nécessaires à l'exécution de leur tâche dans l'organisation : or ceci s'avère contraire au principe prudent de séparation des pouvoirs. Suivant l'ordre de transmission proposé dans RBAC, il peut sembler également étrange que les rôles préférés héritent ainsi aussi des interdictions qui leur proviennent des rôles qui leur sont moins préférés, notamment dans le cas d'une relation de hiérarchie administrative entre rôles : un directeur récupèrerait ainsi toutes les interdictions spécifiées pour ses employés, alors qu'il est censé avoir plus de pouvoirs qu'eux.

19. Dans le cas d'une relation d'autorité hiérarchique, le rôle *directeur* est souvent dit être un rôle *senior*, alors que celui d'employé est dit être un rôle *junior.*

Pour empêcher ces effets non souhaitables, (Cuppens *et al.*, 2004) suggèrent de faire dépendre les sens de transmission des permissions et des obligations de la sémantique de la relation d'ordre exploitée entre les rôles : du rôle le moins spécialisé vers le rôle le plus spécialisé dans le cas d'une relation d'ordre traduisant une qualification technique [20], et des rôles juniors vers les rôles seniors préférés dans le cas d'une relation d'autorité administrative. Le sens de la transmission des interdictions de diffuser une information est le même dans le cas d'un ordre reflétant la compétence technique, mais il va des rôles seniors vers les rôles juniors pour une relation de hiérarchie admi-nistrative : ceci ayant pour but d'éviter que les rôles juniors aient finalement plus de pouvoirs que les rôles senior. Certains auteurs recommandent même de contrôler le sens et la portée des droits de transmission de manière plus fine, voire localement à chaque rôle défini dans l'organisation, en tenant compte aussi de la tâche et de l'orga-nisation concernées. (Feldmeier, 2006) introduit une distance entre les rôles d'une organisation, définie sur la base d'une relation d'ordre permettant de comparer ces rôles, pour limiter la portée de la propagation de la transmission d'un droit. Il va jusqu'à associer des méta-données à chaque permission pour en préciser le champ ; dans son modèle, les droits peuvent être transmis par héritage ou par délégation : (Feldmeier, 2006) précise ainsi quel processus de transmission est associé à chaque droit, ainsi que le rôle (pour une transmission par héritage) ou l'agent (pour une transmission par délégation) initialement détenteurs du droit pour qu'il soit ensuite possible de vérifier qu'une transmission de droit est valide à un instant donné. Le formalisme ainsi proposé permet une grande finesse dans la spécification des modalités de transmission de droits, mais cela est au prix d'une plus grande complexité d'expression.

Le second mode envisagé de transmission de droits repose sur un ordre de composition entre organisations. (Cuppens *et al.*, 2004) suggère que les permissions et les interdictions soient transmises d'une organisation vers les organisations qui la composent, à condition que les rôles concernés soient également définis dans les organisations composantes.

4.2. Transmission des droits d'échange d'informations au sein des organisations avec PEPS-ORG

Nous considérons que (Cuppens *et al.*, 2004) proposent un compromis raisonnable entre les exigences du bon sens, et le besoin d'efficacité et de concision d'expression. Nous avons donc ainsi défini dans PEPS-ORG trois prédicats pour désigner trois natures différentes de relations d'ordre. Si $r1, r2$ sont deux rôles, et $o, o1, o2$ sont trois organisations,

- $Specializes(o, r1, r2)$ signifie que $r1$ est une spécialité technique de $r2$ dans o,
- $Manages(o, r1, r2)$ signifie que $r1$ a autorité administrative sur $r2$ dans o, et
- $Composed(o1, o2)$ signifie que $o2$ est une organisation composante de $o1$.

20. Ainsi, si le rôle de chirurgien est considéré comme spécialisant le rôle de médecin, le rôle de chirurgien hérite des permissions accordées au rôle de médecin par la politique.

Pour une application donnée, les formules construites avec les prédicats $Specializes$ et $Manages$ permettent de décrire respectivement des instances d'ordres de spécialisation technique et d'autorité administrative entre rôles dans une organisation donnée. Le prédicat $Composed$ sert quant à lui à décrire des instances d'ordre de composition entre organisations. Pour une application donnée, l'ensemble de ces formules est ajouté à Σ^{org}, en tant que contraintes contextuelles entre rôles.

Afin de traiter les spécificités et les besoins de certaines applications, nous proposons les axiomes suivants. Soient $r1, r2, r3, r'$ des rôles, et $o, o', o1, o2, o3$ des organisations :

– Pour la transmission de la permission de diffuser de l'information, en fonction de la nature de la relation d'ordre utilisée (spécialisation technique ou autorité administrative) entre les rôles d'une organisation :

AXIOME 5. —
$\forall r1, r2, r', \ \forall o, o',$
$Specializes(o, r1, r2) \wedge P^{org}_{Send}(r2, o, r', o', i) \implies P^{org}_{Send}(r1, o, r', o', i)$
autrement dit : si $r1$ est une spécialité technique de $r2$ dans o, alors toute permission de diffuser accordée à $r2$ l'est également à $r1$.

Cet axiome signifie que $r1$ a au moins les permissions accordées à $r2$, de par sa compétence technique plus poussée que celle de $r2$.

AXIOME 6. —
$\forall r1, r2, r', \ \forall o, o',$
$Manages(o, r1, r2) \wedge P^{org}_{Send}(r2, o, r', o', i) \implies P^{org}_{Send}(r1, o, r', o', i)$
autrement dit : si $r1$ a autorité administrative sur $r2$ dans o, alors toute permission de diffuser accordée à $r2$ l'est également à $r1$.

Cet axiome signifie que $r1$ a plus de permissions que $r2$, de par son autorité administrative sur $r2$. Et, si les rôles définis dans $o1$ le sont également dans $o2$:

AXIOME 7. —
$\forall r, r3, \ \forall o1, o2, o3,$
$Composed(o1, o2) \wedge P^{org}_{Send}(r, o1, r3, o3, i) \implies P^{org}_{Send}(r, o2, r3, o3, i)$
autrement dit : si $o2$ est une organisation composante de $o1$, alors alors toute permission de diffuser accordée à r dans $o1$ l'est également à r dans $o2$.

– Pour la transmission de l'interdiction de diffuser :

AXIOME 8. —
$\forall r1, r2, r, \ \forall o, o',$
$Specializes(o, r1, r2) \wedge F^{org}_{Send}(r2, o, r', o', i) \implies F^{org}_{Send}(r1, o, r', o', i)$

i.e. si $r1$ est une spécialité technique de $r2$ dans o, alors toute interdiction de diffuser attribuée à $r2$ l'est également à $r1$.

Cela est conforme au fait que $r1$ est considéré comme un cas particulier du rôle $r2$.

AXIOME 9. —

$\forall r1, r2, r, \ \forall o, o',$

$Manages(o, r1, r2) \wedge F^{org}_{Send}(r1, o, r', o', i) \wedge \neg Specializes(o, r1, r2)$

$\implies F^{org}_{Send}(r2, o, r', o', i)$

i.e. si $r1$ a autorité administrative sur $r2$ dans o, et si $r1$ n'est pas une spécialité technique de $r2$, alors toute interdiction de diffuser imposée à $r1$ l'est également à $r2$.

Si $r1$ a autorité sur $r2$, il semble naturel de souhaiter que $r1$ ait plus de pouvoirs que $r2$: $r1$ ne doit donc pas hériter des interdictions définies pour les rôles qui lui sont subordonnés. D'où le sens de l'héritage inverse décrit dans l'axiome 9. Mais dans le cas particulier où le rôle subordonné a plus de compétence technique que le rôle de chef (cas de l'existence d'une relation de spécialisation entre le subordonné et son chef), c'est la loi prévue par la relation de compétence technique qui prévaut (axiome 8) car il s'avère souvent plus utile de respecter les compétences techniques que celles liées à un pouvoir hiérarchique (cf 4.1).

Et, si les rôles définis dans $o1$ le sont également dans $o2$:

AXIOME 10. —

$\forall o1, o2, o3, \ \forall r, r3,$

$Composed(o1, o2) \wedge F^{org}_{Send}(r, o1, r3, o3, i) \implies F^{org}_{Send}(r, o2, r3, o3, i)$

autrement dit : si $o2$ est une organisation composante de $o1$, alors toute interdiction de diffuser imposée à r dans $o1$ l'est également à r dans $o2$.

Pour une application donnée, nous proposons à l'utilisateur de choisir un jeu d'axiomes (H^{org}) parmi les axiomes 5...10 ci-dessus pour les ordres définis entre rôles d'organisations, et entre organisations s'il y a lieu.

5. Propriétés de politiques organisationnelles d'échange d'informations

Une fois qu'une politique organisationnelle d'échange d'informations a été exprimée avec PEPS-ORG, il paraît plus efficace de l'analyser au sein de PEPS-ORG : en effet, le nombre d'entités (ici, de rôles et d'organisations) de l'espace de constantes à explorer par le solveur SAT de PEPS étendu au langage PEPS-ORG est *a priori* plus petit [21] que le nombre d'individus peuplant les rôles dans les organisations, et concernés in fine par la politique d'échange d'informations si elle était exprimée en termes d'agents directement avec PEPS - en supposant que l'on ait connaissance de cet ensemble d'agents. Il paraît également plus facile de formuler et comprendre l'expression des

21. Le ratio dépendant de chaque application particulière considérée.

propriétés requises en termes conceptuels de rôles et d'organisations, plutôt qu'en termes d'individus.

Pour analyser une politique, on utilisera le solveur PEPS pour vérifier ses propriétés attendues, exprimées également avec PEPS-ORG.

Suivant la démarche décrite dans (Delmas, Polacsek, 2013), nous avons reformulé des propriétés générales (inconsistance, complétude, applicabilité et minimalité). Nous avons également défini des propriétés plus spécifiques pour empêcher des fuites non autorisées d'informations au travers d'organisations. Nous donnons ci-dessous quelques exemples de ces propriétés.

5.1. Inconsistance

En nous inspirant de (Cholvy, Cuppens, 1997), nous considérons que $OEPS = \langle \Sigma, OEP \rangle$ est inconsistante s'il peut exister une situation dans laquelle il serait à la fois permis et interdit pour un agent d'envoyer une information à un autre, à cause du ou des rôles que les agents émetteur ou destinataire pourraient être amenés à jouer. L'inconsistance peut avoir ici deux types de causes : soit elle est intrinsèque aux règles d'échange d'informations définies dans OEP pour un même rôle émetteur, soit elle peut intervenir s'il est possible pour un agent de jouer deux rôles donnés distincts. Nous allons introduire pas à pas ces idées, en orientant d'abord une première définition sur le rôle émetteur, puis en l'étendant à deux rôles émetteurs compatibles, c'est-à-dire qui peuvent être joués par un même individu dans une organisation (cf 3.1).

DEFINITION 11 (O_{role}-inconsistance). —

Une spécification de politique organisationnelle d'échange OEPS est O_{role}-inconsistante si

$\exists o1, o3, o4 \ \exists r1, r3, r4 \ \exists i, \exists \phi,$

$(\Sigma, OEP, (D^{org}), (H^{org}), \phi) \models$

$P^{org}_{Send}(r1, o1, r3, o3, i) \wedge F^{org}_{Send}(r1, o1, r4, o4, i) \wedge \neg Incompatible(r3, o3, r4, o4)$

où ϕ est une formule PEPS *sans prédicat normatif, qui décrit un type de situation possible.*

Le cas particulier où $r3 = r4$ et $o3 = o4$ correspond au cas le plus intuitif où la politique donne à un rôle émetteur $r1$ à la fois la permission et l'interdiction d'envoyer une information à un même autre rôle destinataire : en effet, $\neg Incompatible(r, o, r, o)$ est toujours vrai (cf 3.1).

Dans le cas général, la dernière composante de cette définition signifie qu'il est possible pour un même agent de jouer les deux rôles $r3$ et $r4$, respectivement dans $o3$ et $o4$. Or dans une situation correspondant à ϕ, la politique lui permettrait d'être destinataire en provenance de $r1$ de l'information i en jouant son rôle $r3$, mais lui interdirait de l'être en jouant son rôle $r4$. Le dilemme auquel peut être confronté un

agent jouant le rôle émetteur $r1$ peut être en effet aussi lié à la compatibilité possible entre deux rôles destinataires différents.

Il revient à l'utilisateur qui définit une politique de juger si l'occurence d'une telle situation de dilemme est réellement envisageable pour l'application considérée. Dans ce cas, il est nécessaire :

– soit de rajouter une contrainte d'incompatibilité entre les rôles récepteurs $r3$ dans $o3$, et $r4$ dans $o4$,

– soit d'introduire un mécanisme de priorité entre règles pour résoudre le conflit localement au niveau du rôle $r1$ (Cuppens *et al.*, 2001),

– soit de modifier OEP dans le but d'obtenir une politique consistante, en enlevant au moins la source d'inconsistance locale au rôle $r1$ ainsi identifiée. Bien sûr, le solveur PEPS n'indique pas comment modifier la politique : mais il indique quelles règles produisent une inconsistance potentielle, ce qui fournit déjà une aide précieuse à l'utilisateur.

DEFINITION 12 (O_{orga}-inconsistance). —

Une spécification de politique organisationnelle d'échange $OEPS$ est O_{orga}-inconsistante si

$$\exists o1, o2, o3, o4 \ \exists r1, r2, r3, r4 \ \exists i, \exists \phi,$$

$$(\Sigma, OEP, (D^{org}), (H^{org}), \phi) \models$$

$$P^{org}_{Send}(r1, o1, r3, o3, i) \wedge F^{org}_{Send}(r2, o2, r4, o4, i)$$

$$\wedge \neg Incompatible(r1, o1, r2, o2) \wedge \neg Incompatible(r3, o3, r4, o4)$$

où ϕ est une formule PEPS *sans prédicat normatif, qui décrit un type de situation possible.*

Autrement dit, dans une situation répondant à la description ϕ, tout agent pouvant jouer les deux rôles $r1$ dans $o1$ et $r2$ dans $o2$ serait confronté à un dilemme en cas de connaissance de l'information i. Cette forme d'inconsistance est dûe au fait qu'un même agent peut jouer plusieurs rôles soit en tant qu'émetteur de l'information, soit en tant que récepteur. Pour remédier à cette source d'inconsistance, si un mécanisme de gestion de priorités entre règles n'a pas été défini, le concepteur de la politique d'échange peut :

– soit rajouter une contrainte d'incompatibilité entre rôles dans Σ^{org}, pour empêcher qu'un même agent puisse jouer les deux rôles $r1$ dans $o1$ et $r2$ dans $o2$,

– soit rajouter une contrainte de rôle dans Σ^{org}, pour rendre $r3$ dans $o3$ et $r4$ dans $o4$ incompatibles,

– soit modifier OEP,

– soit, si cela s'avère contrôlable, s'assurer qu'une situation de type ϕ ne puisse jamais arriver.

5.2. Complétude

Une spécification de politique organisationnelle d'échange est dite complète si dans *tous* les cas elle spécifie si les agents ont l'obligation, la permission ou l'interdiction d'envoyer des informations à d'autres dès qu'ils en ont connaissance, de manière à éviter ce qui s'apparente à une situation de vide juridique : en général, il est très coûteux d'exiger cette propriété, et c'est probablement inutile. Pour une organisation donnée, il semble souvent plus judicieux de limiter le champ souhaité de la complétude aux thèmes d'intérêt pour l'organisation (Cholvy *et al.*, 2006 ; 2007). C'est pourquoi nous définissons d'abord une version assez restrictive de la propriété de complétude : pour un rôle dans une organisation, une spécification de politique organisationnelle d'échange $OEPS$ est complète pour un thème donné si elle est complète pour toute information concernant ce thème.

Soient Ω un ensemble d'organisations pour lesquelles $OEPS$ a été spécifiée, o une organisation dans Ω, et T un thème donné (constante de la sorte $\mathcal{T}$).

DEFINITION 13 ($O_{role} - T$-complétude). —

$OEPS$ est $O_{role} - T$-complète dans Ω pour le rôle r dans l'organisation o si

$\forall o' \in \Omega, \quad \forall r', \quad \forall i,$

$(\Sigma, OEP, (D^{org}), (H^{org})) \models$

(Topic(i, T) $\Longrightarrow$ $O^{org}_{Send}(r, o, r', o', i) \vee P^{org}_{Send}(r, o, r', o', i) \vee F^{org}_{Send}(r, o, r', o', i))$

Supposons de plus que toutes les organisations d'Ω partagent l'usage d'une ontologie métier Θ de thèmes.

DEFINITION 14 ($O_{role} - \Theta$-complétude). —

$OEPS$ est $O_{role} - \Theta$-complète dans Ω pour le rôle r dans o, si pour tout thème de Θ, elle est $O_{role} - T$-complète dans Ω pour r dans o.

DEFINITION 15 ($O_{orga} - \Theta$-complétude). —

$OEPS$ est $O_{orga} - \Theta$-complète dans Ω pour l'organisation o, si elle est $O_{role} - \Theta$-complète dans Ω pour tous les rôles définis dans o.

5.3. Perméabilité d'information à travers des organisations

Dans les systèmes de surveillance pour des applications critiques, il est nécessaire de protéger certaines informations parce que leur divulgation pourrait mettre à mal des savoir-faire techniques qui doivent rester confidentiels, ou encore parce que leur divulgation pourrait induire de la panique dans la population. C'est pourquoi nous souhaitons détecter dans la couche PEPS-ORG la possibilité de diffusion d'information non autorisée à travers les organisations, à cause de la compatibilité de deux rôles dans une ou des organisations, c'est-à-dire qu'un même agent pourrait jouer ces deux rôles (cf 3.1) , et éventuellement servir ainsi de relais incontrôlable pour l'information.

Soit Ω un ensemble d'organisations pour lesquelles a été définie une spécification de politique organisationnelle d'échange d'information $OEPS$.

DEFINITION 16 (O-information perméabilité). —

$OEPS$ est O-information perméable pour Ω si, bien qu'elle ne soit pas O_{role}-inconsistante,

$$\exists i,\ \exists o_1 \in \Omega, \exists o_n \in \Omega,\ \ \exists r_1, r_n,$$

$$(\Sigma, OEP, (D^{org}), (H^{org})) \models F^{org}_{Send}(r_1, o_1, r_n, o_n, i) \wedge TransP^{org}_{Send}(r_1, o_1, r_n, o_n, i)$$

où $TransP^{org}_{Send}(r_1, o_1, r_n, o_n, i)$ signifie que, selon $OEPS$, i pourrait être transmise de r_1 dans o_1 vers r_n dans o_n via des agents pouvant servir de relais entre organisations.

$TransP^{org}_{Send}$ est définie pas à pas comme suit :

1. $TransInterne^{org}$: Transmission permise d'information au sein d'une organisation :

$\forall o,\ \forall r, r',\ \forall i$:

$TransInterne^{org}(o, r, r, i)$

$P^{org}_{Send}(r, o, r', o, i) \implies TransInterne^{org}(o, r, r', i)$

$P^{org}_{Send}(r, o, x, o, i) \wedge TransInterne^{org}(o, x, r', i) \implies TransInterne^{org}(o, r, r', i)$

i.e. selon la politique, la transmission de i est autorisée pas à pas du rôle r vers le rôle r' à l'intérieur de l'organisation o.

2. $Link^{org}$: Exhibition d'un pont ou relais entre deux organisations pour une information

$\forall o, o',\ \forall r, r',\ \forall i,$

$\neg Incompatible(r, o, r', o') \vee P^{org}_{Send}(r, o, r', o', i) \implies Link^{org}(r, o, r', o', i)$

i.e. i pourrait être envoyée de l'organisation o à l'organisation o', soit parce qu'un agent qui ne séparerait pas rigoureusement ses fonctions jouerait un rôle dans o et o', soit parce que cette transmission est autorisée explicitement par la politique.

3. $TransP^{org}_{Send}$: Diffusion d'information autorisée dans et entre des organisations

$\forall o, o_1, o_2, o_n,\ \forall rs, rr, rs_1, rr_1, rs_2, rr_2, rs_n, rr_n,\ \forall i$:

$$TransInterne^{org}(o, rs, rr, i) \implies TransP^{org}_{Send}(rs, o, rr, o, i)$$
$$TransInterne^{org}(o_1, rs_1, rr_1, i) \wedge Link^{org}(rr_1, o_1, rs_2, o_2, i)$$
$$\wedge\ TransP^{org}_{Send}(rs_2, o_2, rr_n, o_n, i)$$
$$\implies TransP^{org}_{Send}(rs_1, o_1, rr_n, o_n, i)$$

i.e. l'information i pourrait être envoyée d'un premier rôle émetteur rs_1 de l'organisation o_1, vers un dernier rôle récepteur rr_n dans o_n, via des règles d'obligation ou de permission d'échange de l'information de la politique.

Afin de prévenir une telle fuite d'information, l'utilisateur peut rendre des rôles incompatibles entre des organisations d'Ω, en modifiant alors des contraintes de domaine dans Σ^{org}. Il peut aussi modifier la politique organisationnelle d'échange d'informations OEP.

Notons que cette définition pourrait être généralisée en faisant intervenir la notion de compatibilité entre rôles émetteurs, ou entre rôles récepteurs, comme fait en 5.1 concernant la propriété d'inconsistance : mais cela n'aiderait pas à la compréhension du principe essentiel.

Nous avons donc montré qu'en introduisant les concepts de rôle et organisation, nous pouvons utiliser PEPS pour raisonner sur la possibilité de fuite d'information sans avoir à envisager explicitement la question au niveau des agents individuels qui appartiennent aux organisations. Nous pouvons ainsi proposer d'anticiper les risques en orientant l'utilisateur vers des recherches au préalable de solutions concernant la définition de la structure des organisations.

Le gain espéré réside en une analyse à un niveau d'abstraction plus adéquat pour l'utilisateur, et une moindre complexité de calcul car le nombre d'entités de types rôle et organisation est en général inférieur à celui des agents employés dans les organisations concernées. Les analyses de propriétés ainsi menées reposent également sur la seule connaissance des rôles et des organisations, sans doute plus disponible que celles des agents.

En termes de complexité de calcul pour les analyses de vérification des propriétés, il est difficile de donner une estimation générale des ratios des deux indicateurs :

– nombre de règles de la politique exprimées en PEPS-ORG *versus* en PEPS,

– nombre d'agents individuels *versus* nombre de rôles et d'organisations pour une politique selon qu'elle soit exprimée avec les concepts natifs de PEPS, ou avec ceux de PEPS-ORG :

cela dépend des applications concernées.

6. Conclusion et futurs travaux

Les systèmes d'informations critiques sont souvent partagés au sein d'organisations, ou entre organisations. Nous avons expliqué pourquoi il serait donc plus efficace de définir et analyser leur politique d'échange d'informations au niveau des organisations plutôt qu'à celui des agents individuels jouant des rôles dans ces organisations, afin de gagner la confiance des utilisateurs.

Partant de l'environnement formel PEPS, nous l'avons enrichi avec PEPS-ORG, une couche indépendante au-dessus du langage natif de PEPS, pour pouvoir permettre d'exprimer et d'analyser des spécifications de politiques d'échange au niveau organisationnel. Les principales contributions de ce travail sont les suivantes. D'abord, il est possible d'exprimer de manière distincte, dans cette couche de langage PEPS-ORG, les contraintes métier portant sur les rôles dans les organisations, et les politiques orga-

nisationnelles d'échange. Par ailleurs, nous avons proposé une méthode pour rendre l'expression de politiques plus concise, en proposant des jeux d'axiomes de transmissions des droits en matière de diffusion d'information entre rôles ou organisations, que l'utilisateur doit choisir en fonction des caractéristiques de l'application visée.

Avec PEPS-ORG, nous avons redéfini des propriétés générales et classiques sur les politiques, mais aussi une propriété plus spécifique pour empêcher les fuites d'informations non autorisées. Nous espérons tirer profit du solveur PEPS pour analyser facilement des politiques organisationnelles : cette expérimentation reste à faire.

Notre approche est prudente : si une politique organisationnelle ne vérifie pas une propriété décrite au niveau organisationnel, nous suggérons d'anticiper tout problème en modifiant soit la politique, soit certaines contraintes dans les organisations de l'application considérée : même si en réalité, nous ignorons si une situation redoutée qui mettrait la propriété en défaut se présentera un jour avec une information réelle.

Le langage PEPS (et donc PEPS-ORG) peut donner lieu à d'autres extensions : par exemple, il serait utile d'introduire le temps pour permettre d'exprimer et de raisonner sur des contraintes temporelles concernant les périodes où est joué un rôle. Le langage PEPS-ORG gagnera à être enrichi par de nouveaux concepts, comme la notion de contexte relatif à une organisation, pour pouvoir conditionner un droit de transmettre une information.

La contribution de ce travail va au-delà d'une simple extension du langage PEPS : nous avons proposé ici une méthodologie pour formaliser les échanges d'informations entre organisations. Cette méthodologie devrait parfois inciter les utilisateurs à s'interroger sur la nature réelle de la structure des organisations dont il s'agit de réglementer les échanges d'informations : un autre résultat espéré est donc l'obtention de définitions plus précises et plus pertinentes des organisations, *in fine* plus fiables pour la garantie de propriétés requises sur les échanges d'informations.

Remerciements

Nous remercions Laurence Cholvy, Rémi Delmas, Olivier Poitou et Thomas Polacsek pour leurs commentaires et suggestions à la source d'améliorations de cet article. Ce travail a été financé par le projet ONERA MAPEIS.

Bibliographie

Benferhat S., Kalam A. A. E., Miège A., Baida R. E., Cuppens F., Saurel C. *et al*. (2003). Organization Based Access Control. In *IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003).*

Carmo J., Pacheco O. (2001). Deontic and action logics for organized collective agency, modeled through institutionalized agents and roles. *Fundamental Informaticae*, vol. 48(2,3), p. 129â163.

Chellas B. F. (1980). *Modal logic : an introduction*. Cambridge, Cambridge Univ. Press.

Cholvy L., Cuppens F. (1997). Analyzing consistency of security policies. In *IEEE Symposium on Security and Privacy*, p. 103-112.

Cholvy L., Garion C., Saurel C. (2006). Information sharing policies for coalition systems. In *NATO RTO-IST-062 Symposium on dynamic communications management.*

Cholvy L., Garion C., Saurel C. (2007). ModÃ©lisation de rÃ©glementations pour le partage d'information dans un systÃ¨me multi-agents. In *Actes des quatriÃ¨mes journÃ©es francophones modÃ¨les formels de l'intercation (mfi'07).*

Crampton J. (2003). On permissions, inheritance and role hierarchies. In *10th ACM conference on Computer and Communication Security*, p. 85-92.

Cuppens F., Cholvy L., Saurel C., Carrère J. (2001). Merging regulations: analysis of a practical example. *Data and Knowledge Fusion, Special issue of International Journal of Intelligent Systems*, vol. 16.

Cuppens F., Cuppens-Boulahia N., Miège A. (2004). Héritage de privilèges dans le modèle OrBAC : application dans un environnement réseau. In *SSTIC 04 : Symposium sur la Sécurité des Technologies de l'Information et des Communications.*

Delmas R., Polacsek T. (2013). Formal methods for exchange policy specification. In *Proceedings of Conference on Advanced Information Systems Engineering (CAiSE)*, p. 288-303.

Feldmeier C. J. (2006). *Limiting hierarchical inheritance of permissions in access control model*. Rapport technique. Fairfax, USA, George Mason University, ISA 767 Secure electronic commerce.

Glassey O., Chappelet J.-L. (2002). *Comparaison de trois techniques de modélisation de processus : ADONIS, OSSAD et UML.* Rapport technique. UER Management public / systèmes d'informations, Lausanne, Working paper de l'IDHEAP/14.

Kalam A. A. E., Balbiani P., Benferhat S., Cuppens F., Deswarte Y., Baida R. E. *et al*. (2003). Modèles et politiques de sécurité des systèmes d'information et de communication en santé et social. *Santé et Systémique*, vol. 7, p. 107-125.

Mandl K., Overhage J., Wagner M., al. (2004). Implementing syndromic surveillance : a practical guide informed by early experience. *American Medical Informatics Association*, vol. 11(2), p. 141-150.

Pacheco O., Carmo J. (2003). A Role Based Model for the normative specification of organized collective agency and agent interaction. *Journal of Autonomous Agents and Multi-Agent Systems*, vol. 6, p. 145-184.

Parks L. I. (2004). Homeland security and HIM. appendix b : syndromic srveillance systems in bioterrorism and outbreak detection. *Journal of AHIMA 75 (American Health Information Management Association)*, vol. 6.

Rozière P. (2004). *Logique mathématique : introduction*. Rapport technique. Paris 7, MT 3062.

Sandhu R., Coyne E., Feinstein H., Youman C. (1996). Role-Based Access Control models. *IEEE Computer*, vol. 29(2), p. 38-47.

von Wright G. H. (1951). *Deontic logic*.