Manuscrit présenté pour l'obtention de l'

Habilitation à diriger les recherches

De l'Université Toulouse 3 Paul Sabatier

Spécialité : Informatique

par

Romain LABORDE

Institut de Recherche en Informatique

Ecole Doctorale Mathématiques, Informatique et Télécommunications de Toulouse

Contributions à la gestion de la sécurité des infrastructures virtuelles

Présentée le 17 Juin 2016

JURY

Maryline LAURENT	Professeur, Telecom SudParis
Francine KRIEF	Professeur, Bordeaux INP
Frédéric CUPPENS	Professeur, Telecom Bretagne
Abdelmadjid BOUABDALLAH	Professeur, Université de Technologie de Compiègne
Abdelmalek BENZEKRI	Professeur, Université Toulouse 3 Paul Sabatier

Résumé

L'adoption massive de systèmes informatiques multiples et variés dans les entreprises et dans les foyers a profondément changé les activités humaines exacerbant par là même les problématiques de sécurité.

En effet, si auparavant le système d'information était cloisonné au sein des murs de l'entreprise et uniquement accessible aux employés au travers d'équipements propres à l'entreprise, la situation est bien différente aujourd'hui. Les entreprises s'allient pour répondre plus efficacement à des opportunités métier et donc désirent partager des ressources facilement mais de manière contrôlée. Les services informatiques se sont dématérialisés et externalisés. Les usages des employés ont aussi évolué. Le télétravail s'est développé et les employés veulent utiliser leurs équipements personnels pour accéder aux actifs de l'entreprise.

En même temps, l'informatique a pénétré les habitations domestiques. D'un simple ordinateur connecté par un modem, le réseau domestique est aujourd'hui constitué d'une multitude d'équipements. Les objets du quotidien étant devenus de véritables ordinateurs, les contours même des réseaux informatiques domestiques ont aussi largement dépassé les murs des habitations. En parallèle, la vie des usagers s'est numérisée et les transactions électroniques se sont généralisées.

Dans ce contexte se pose la question suivante : Comment gérer la sécurité d'une infrastructure informatique devenue virtuelle, créée à la demande, dynamique et dont, clairement, les contours ne peuvent plus être tracés sur une carte ? Cet enjeu concerne aussi bien les entreprises que les particuliers.

Les travaux de recherche que nous menons depuis une dizaine d'années tentent d'apporter des réponses à cette question en traitant les problématiques liées à l'expression, l'analyse et le déploiement de politiques de sécurité. Notre approche est construite autour de deux paradigmes : le modèle de contrôle d'accès basé sur les attributs et l'architecture de gestion à base de politiques. En utilisant ces deux briques, nous avons apporté des contributions pour faciliter la gestion de politiques de sécurité dynamiques, adaptables, compréhensibles, multi-administrées.

Table des matières

Liste des figures

Chapitre 1. Introduction

Ce document propose un résumé de mes activités de recherche. Ma formation de recherche (DEA puis thèse) s'est effectuée au sein de l'équipe SIERA (Administration de Réseaux Et Intégration de Services). Durant ces années, j'ai travaillé sur les problématiques de gestion de la sécurité réseau. En novembre 2005, j'ai intégré l'équipe ISSRG (Information Systems Security Research Group) du Pr. D. W. Chadwick de l'université du Kent à Canterbury (Royaume-Uni) en tant que chercheur associé. Mes activités de recherche se sont alors ouvertes vers la gestion des autorisations sur les systèmes d'information. Depuis mon retour dans l'équipe SIERA en tant que Maître de conférence, j'ai combiné ces expériences dans l'objectif de proposer des solutions de gestion considérant la notion de sécurité de manière plus globale, c'est à dire incluant les aspects réseau, système et service. Dans ce document, je présente mes résultats de recherche obtenus à partir de mon installation au poste de maître de conférence. Les informations avant cette date ne sont données que pour comprendre le parcours que j'ai suivi.

Si le document que je présente ici est personnel, il est évident que le travail de recherche synthétisé a été effectué conjointement avec différents collègues, principalement des membres de mon équipe.

1.1 Problématique de la gestion de la sécurité

Le 26 septembre 2005, je terminais ma soutenance de thèse de doctorat intitulée « Un cadre formel pour le raffinement de l'information de gestion de sécurité réseaux: Expression et Analyse » en présentant mes propositions de travaux futurs dans une dernière diapositive (Figure 1). J'avais décomposé l'information de gestion de la sécurité en trois niveaux d'abstraction : les objectifs de sécurité réseau qui proviennent de choix stratégiques, les tactiques de sécurité réseau qui sont les choix conceptuels d'une solution de sécurité réseau et enfin les configurations sur les équipements. Mon travail avait porté sur l'expression et l'analyse de chaque niveau ainsi que les problèmes de raffinement entre les niveaux d'abstraction. Dans cette dernière diapositive j'envisageais de pouvoir contrôler automatiquement le niveau configuration par le niveau tactique (flèche contrôle). Je voulais aussi capturer les données provenant de l'activité de surveillance (flèche surveillance) afin de vérifier que le niveau tactique était toujours réalisé mais aussi de déterminer l'impact qu'un incident peut avoir sur les objectifs de sécurité.

J'ai continué à me poser ces questions dans la suite de ma carrière : Comment exprimer une solution de sécurité ? Comment l'analyser ? Comment la déployer ?

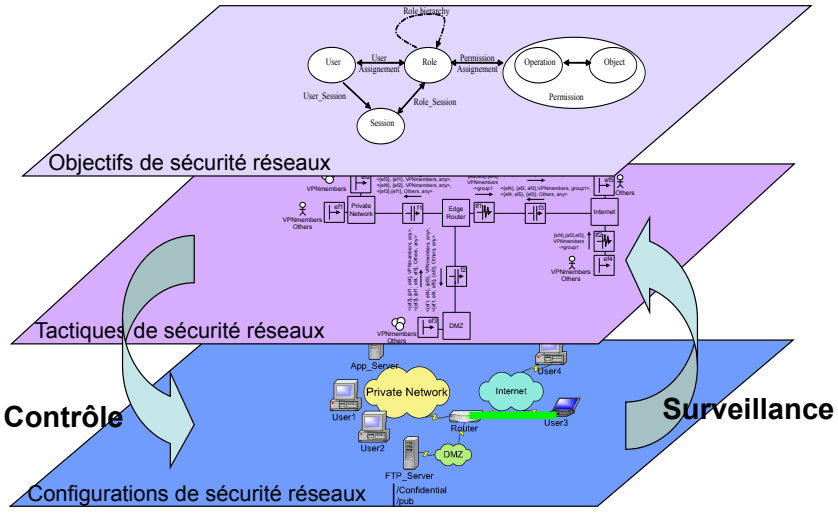


Figure 1. Ma vision d'une boucle de gestion de la sécurité à la fin de ma thèse

L'expression de politiques de sécurité traite de la définition des contours que l'on désire dessiner pour l'infrastructure que l'on contrôle. Mais alors, quels contours sommes-nous capables de dessiner ? Il faut que la capacité d'expression des langages de politique de sécurité soit suffisante pour spécifier les objectifs mais aussi la manière de les réaliser. La problématique de l'analyse porte elle sur la nature même des contours de notre infrastructure. N'y a-t-il pas de conflit ? Est-ce que les contours qui ont été dessinés sont les bons ? Enfin le problème de déploiement vise l'automatisation de la mise en œuvre d'une politique de sécurité. Comment déployer ce qui a était exprimé dans un environnement qui change lui-même. Comment réadapter un déploiement pour que les objectifs de sécurité soient toujours atteints ? Ces questions se sont révélées de plus en plus complexes. En effet, si auparavant le système d'information était cloisonné au sein des murs de l'entreprise et uniquement accessible aux employés au travers d'équipements propres à l'entreprise, la situation est bien différente aujourd'hui. Les contours physiques de l'infrastructure réseau de l'entreprise ont explosé. Les employés ne travaillent plus uniquement dans les murs de l'entreprise. Ils peuvent, par exemple, faire du télétravail depuis chez eux ou lors d'un déplacement chez un client. De plus, les entreprises acceptent aujourd'hui que les employés utilisent leurs propres équipements pour se connecter au réseau de l'entreprise ; phénomène connu sous le nom de Bring Your Own Device (Harkins 2012). Les équipements d'accès au capital de l'entreprise ne sont donc plus exclusivement dédiés. Les besoins de collaboration entre entreprises ont aussi ouvert les réseaux afin de faciliter les échanges numériques entre elles. Pour répondre à des projets ou des opportunités métier, les entreprises veulent aujourd'hui pouvoir mettre en place des équipes inter-entreprises rapidement. L'infrastructure informatique support de ces collaborations doit être assez flexible pour répondre à la dynamicité de ces équipes et permettre à un nouveau membre d'intégrer un tel groupe de travail ou de le quitter en fonction des compétences requises à chaque phase du projet. Cela demande aussi que les services soient dématérialisés afin que les participants puissent accéder aux données et logiciels mis en communs

(Harry 2013). Depuis quelques années, les murs des entreprises se sont aussi déportés dans les nuages. Pour des raisons de coût, il peut être plus intéressant pour une entreprise de louer une partie voire même toute son infrastructure que de la posséder.

D'où la conclusion suivante : Comment gérer la sécurité d'une infrastructure informatique devenue virtuelle, créée à la demande, dynamique et dont, clairement, les contours ne peuvent plus être tracés sur une carte ?

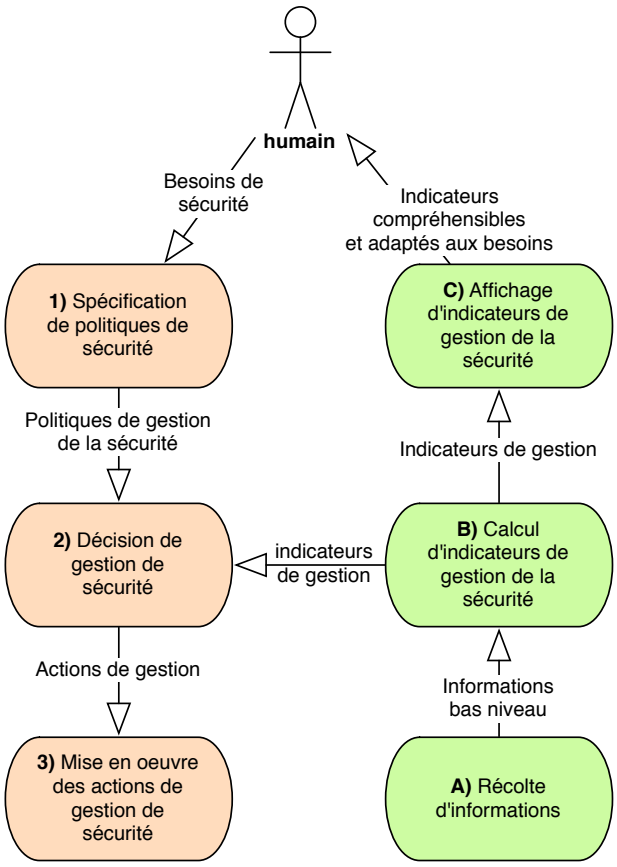


Figure 2. Ma vision d'une boucle de gestion de la sécurité aujourd'hui

L'évolution de la problématique de gestion de la sécurité ainsi que mes recherches effectuées dans ce domaine m'ont amené à affiner ma vision de ce que peut être la boucle de gestion de la sécurité (Figure 2). Tout d'abord, il y a les être humains qui désirent contrôler l'environnement cible. Il est important de considérer explicitement cette entité car selon les cas il peut s'agir d'un administrateur, de plusieurs administrateurs ou encore d'un particulier non informaticien. Cette entité humaine a des besoins de sécurité. Ces besoins de sécurité peuvent être explicitement définis dans des documents de manière formelle ou non. Ils peuvent aussi être implicites, non clairement définis et non documentés. Ces besoins sont traduits dans des politiques de sécurité qui seront transformées au travers d'un processus de raffinement en actions de gestion sur l'environnement cible (éléments orangés sur la gauche de la Figure 2). Pour cela, les politiques sont traitées à un niveau indépendant des technologies afin de prendre des décisions de gestion (Etape 2). Les décisions de gestion vont engendrer des actions de gestion sur l'environnement à contrôler qui seront mises en œuvre par des

mécanismes particuliers (Etape 3). Les mécanismes de mise en œuvre des actions de gestion sont eux dépendants des technologies gérées. Le processus de raffinement de politiques de sécurité est complété par un processus de supervision de l'environnement géré (éléments verts sur la droite de la Figure 2). Des données sur l'état du système géré, son environnent sont récoltées (Etape A). Les données récoltées sont alors traitées pour calculer des indicateurs de gestion de la sécurité (Etape B). J'utilise le mot indicateur pour exprimer le fait que le traitement sur les données brutes doit apporter une sémantique à l'information permettant de l'utiliser dans le processus de prise de décision. Ceci a pour objectif de dynamiser la gestion de la sécurité. Enfin, des indicateurs peuvent être présentés à l'utilisateur humain (Etape C). Il est nécessaire de filtrer/transformer ces informations de telle manière que les indicateurs présentés lui donnent la bonne information au bon moment.

Mes travaux de recherche se situent tous dans le cadre de cette boucle de gestion. Je m'en servirai donc comme fil rouge tout au long de ce document.

1.2 Gestion de la sécurité des infrastructures virtuelles

Lors de ces dix dernières années, mes travaux de recherche ont traité de la problématique de gestion de la sécurité selon différents points de vue et terrains d'expérimentation.

Tout d'abord, je me suis intéressé à la gestion des identités et des accès dans les infrastructures virtuelles. Ces travaux ont constitué la continuité de mes travaux de post-docs où j'avais participé au projet d'infrastructure de gestion de privilèges PERMIS[1]. PERMIS offre un langage pour exprimer des politiques d'autorisation de type RBAC. Il permet aussi de définir des contraintes sur l'émetteur d'un rôle ce qui est très intéressant dans le cadre de collaborations car cela permet de définir quelle entreprise peut définir quel rôle dans la collaboration. Cependant, nous nous sommes rapidement trouvés bloqués par le langage de PERMIS. En effet, nous avons eu besoin de définir des contraintes de sécurité que le modèle RBAC ne permettait pas d'exprimer. Comme le langage de PERMIS est lié au modèle RBAC, nous ne pouvions exprimer dans le formalisme de PERMIS nos politiques d'autorisation dynamique. L'expression de politiques de sécurité a été très largement étudiée et un grand nombre de modèles de contrôle d'accès ont été proposés. Les premiers modèles avaient pour ambition de garantir qu'une politique exprimée respectait bien une propriété de sécurité. Par exemple, le modèle de Bell-Lapadula (Bell et al. 1973) pour la confidentialité, les modèles de Biba (Biba 1977) ou de clark et Wilson (Clark et al. 1987) pour la propriété d'intégrité. Depuis le modèle RBAC (Role Based Access Control) (Ferraiolo et al. 1995), les modèles de contrôle d'accès n'ont plus été généralistes. Ils se sont spécialisés présentant i) des concepts intéressants (Barker utilise le terme catégories (Barker 2009)) à considérer pour des cas d'utilisation particuliers, ii) la manière de les manipuler et iii) d'écrire des politiques selon ces concepts. Une multitude de modèles de contrôle d'accès a fleuri fournissant des outils pour exprimer des contraintes de sécurité selon les besoins

[1] http://sec.cs.kent.ac.uk/permis/index.shtml

émergeant (la mobilité, le contexte temporel, la vie privée, etc.). Etant donné qu'il est difficile d'anticiper les usages du futur, ces nouveaux modèles de contrôle d'accès doivent être renouvelés ou mis à jour constamment. Ceci m'a amené à une première constatation : le langage pour exprimer des règles de sécurité doit être indépendant de tout modèle de politique. Les modèles de contrôle d'accès sont utiles comme patrons de conception de politiques de contrôle d'accès de la même façon que l'on utilise des patrons de conception dans le domaine du génie logiciel. C'est pour cela que je préfère utiliser le terme de modèle de politique de contrôle d'accès plutôt que modèle de contrôle d'accès. Cette indépendance vis à vis des modèles de politiques de contrôle d'accès a pu être obtenue grâce à l'approche ABAC (Attribute Based Access Control - (NIST ABAC 2015)) où tout élément significatif en terme de sécurité peut être considéré comme un attribut. En complément, je me suis beaucoup intéressé aux systèmes de gestion à base de politiques (PBMS : Policy Based Management Systems) pour déployer ces politiques. Dans l'architecture PBMS, la logique de gestion est externalisée de l'élément géré au travers de deux agents de gestion : Le point de prise de décision (PDP) qui décide des actions de gestion/de contrôle d'accès à réaliser, et le point d'exécution de la politique (PEP) qui met en œuvre les actions de gestion décidées par le PDP. Cette architecture est simple et permet au langage de politique d'être indépendant de l'élément géré. Nous avons donc pu proposer des solutions de gestion des identités et des accès en couplant l'expression de politique en ABAC avec l'architecture de gestion à base de politique. Les attributs étant les éléments de base de la prise de décision pour les accès, nous avons aussi traité du problème de la gestion de la confiance dans les attributs. Le chapitre 2 aborde ces aspects de ma recherche.

Ce premier axe de recherche nous a permis de définir un cadre méthodologique pour définir conceptuellement une solution de gestion des identités et des accès qui s'adapte à la fois aux besoins de sécurité mais aussi à l'environnement à gérer. En parallèle, nous avons cherché à réaliser une implémentation d'un système de gestion à base de politique qui puisse elle aussi s'adapter dynamiquement aux changements qui pourraient intervenir. En effet, pour qu'un langage puisse s'adapter aux besoins d'expression des politiques de sécurité, celui-ci doit être extensible. Par transitivité, les mécanismes qui prennent des décisions par rapport aux politiques de sécurité doivent être eux aussi adaptables afin qu'ils puissent comprendre les extensions du langage. Les éléments qui mettent en œuvre la politique de sécurité sur l'environnement géré doivent également s'adapter afin de garantir que toute politique de sécurité puisse être appliquée. Ainsi, il faut garantir dans une architecture de gestion à base de politique que, quelle que soit la politique, 1) le PDP sait évaluer la politique et 2) le PEP sait mettre en œuvre les décisions résultantes de cette politique. Nous nous sommes donc intéressés à la problématique d'adaptation d'un système de gestion de sécurité et avons proposé une architecture logicielle dynamiquement adaptable pour la gestion de la sécurité. Ce point est présenté dans le chapitre 3.

La gestion de la sécurité réseau peut être vue comme une fonction distribuée qui implique la coordination d'un ensemble d'équipements possédant chacun des capacités et des services de sécurité

spécifiques. Chaque équipement (terminal ou intermédiaire) impliqué dans la sécurité requiert une configuration précise qui détermine à la fois le comportement local de l'équipement et la sécurité globale du réseau. Il faut donc contrôler la cohérence de ces configurations de sécurité pour garantir le niveau de sécurité globale des composants interconnectés. Dans la continuité de mes travaux de thèse, j'ai travaillé sur la validation formelle de configurations de sécurité réseau. Cette activité est nécessaire dans le processus de raffinement de politiques de sécurité en configurations sur l'environnement géré mais aussi lors de l'investigation d'un problème réseau. Cependant, face à l'innombrable quantité de protocoles implémentés, de mécanismes de sécurité déployés et configurables par de multiples paramètres, comment s'assurer qu'une configuration est non-conflictuelle ? Pour répondre à cette question, nous avons réutilisé notre expérience dans la gestion des identités et des accès où nous avons démontré la capacité d'expression de l'approche ABAC. Nous avons donc proposé un formalisme dans lequel un flux de données est représenté par une encapsulation particulière d'attributs et un mécanisme de sécurité est vu comme étant un traitement spécifique sur ces flux de données ; un mécanisme possède sa propre capacité de traitement et sa propre configuration. En utilisant les Réseaux de Petri colorés hiérarchiques, nous pouvons ainsi représenter et analyser divers mécanismes de sécurité avec leurs configurations ainsi que différentes encapsulations de protocoles. Ces éléments sont décrits dans le chapitre 4.

1.3 Problématiques de la gestion de la sécurité chez les particuliers

Avec les attaques toujours plus nombreuses sur les équipements des particuliers et les problèmes d'atteinte à la vie privée (Petrie et al. 2015), j'ai désiré orienter une partie de mes activités de recherche dans l'optique d'offrir des solutions de gestion de la sécurité pour les particuliers. Appliquer des solutions de gestion aux particuliers pose un problème de fond qui provient de deux hypothèses que nous avions implicitement prises jusque-là et qui ne sont plus valides dans ce contexte:

1) L'interconnexion des infrastructures d'entreprises correspond à un monde fermé dans lequel les entités se connaissent.
2) Les entreprises possèdent des personnels compétents dans la gestion de la sécurité ou à défaut peuvent s'offrir un service pour effectuer cette tâche.

Or un particulier navigue dans un monde ouvert. Il ne connaît pas physiquement les entités à qui il doit faire confiance. Comment connaître le niveau de sécurité d'un site marchand ? Comment savoir si un antivirus est bon ? Il ne connaît pas non plus les entités qui lui fournissent des recommandations sur d'autres entités. Comment savoir si les avis indiquant qu'un antivirus est bon, trouvés sur un forum, sont eux-mêmes bons ? Dans ce cadre là, comment créer un cercle de confiance ? Nous avons travaillé sur la gestion de la confiance des certificats électroniques. A l'origine le problème m'est apparu en observant ma compagne. Celle-ci voulait se connecter sur un site marchand avec le navigateur Firefox. Cependant, un message d'erreur lui indiquait que le certificat de ce site n'était pas émis par une autorité de confiance. A ce moment, elle s'est reconnectée sur le même site avec le

navigateur Safari en me disant que « ce site ne marche qu'avec Safari ». En effet, aucun message d'erreur lié au certificat n'était apparu en utilisant ce navigateur. Il est intéressant de rappeler que i) les certificats électroniques et les infrastructures de gestion de clés (PKI) sont la base de nos outils de sécurité, ii) que les solutions de PKI sont complexes techniquement et technologiquement, et que iii) le marché des PKI (Arnbak et al. 2014) représente des centaines millions de dollars (357.4 million $ en 2013[2] selon l'analyse de l'agence Frost et Sullivan). Dans un premier temps, nous avons investigué ce problème avec pour objectif d'informer les utilisateurs. Cependant, nous nous sommes rendus compte que le problème de certificat validé différemment par des navigateurs était dû à un problème conceptuel dans la gestion de la confiance. Nous avons donc proposé un nouveau modèle que nous souhaitons plus juste envers les utilisateurs. Ce modèle a été accepté par la communauté PKI car il est aujourd'hui inclus dans le brouillon de la prochaine version de la norme ITU-T X.509. Le chapitre 5 détaille ces travaux.

Notre deuxième hypothèse concernant l'existence d'un administrateur sécurité est aussi caduque quand on veut appliquer une solution de gestion de la sécurité aux particuliers car la majorité des particuliers ne sont pas compétents en sécurité. Dans ce monde ouvert, ils n'ont pas non plus dans leur entourage un expert en sécurité qui pourrait les aider dans cette tâche. Or, les particuliers possèdent de plus en plus d'équipements. Ces équipements offrent de plus en plus de fonctionnalités et sont de plus en plus connectés. Aujourd'hui, ma tablette dialogue avec mon smartphone qui communique avec ma chaîne HIFI et mon serveur de sauvegarde ou encore ma télévision, etc. Petit à petit, les réseaux personnels privés se rapprochent de plus en plus des réseaux d'une petite PME. Cet état de fait ne peut que s'amplifier dans l'Internet des Objets. Pour contrôler un tel environnement, il faudra que le particulier définisse sa propre politique de sécurité et qu'il puisse la déployer de la même manière que sur un réseau de PME. Or, on ne peut pas demander à un particulier de comprendre un ou plusieurs modèles de politique de contrôle d'accès et de spécifier sa politique en ABAC. Même imposer l'utilisation d'un modèle de politique de contrôle d'accès est complexe pour un particulier. En effet, les modèles modernes limitent la complexité du nombre de règles par l'utilisation d'abstractions (par exemple, le rôle pour l'utilisateur dans RBAC (Ferraiolo et al. 2003), l'activité/vue pour OrBAC (Kalam et al. 2003), l'intention abstraite dans PBAC (Byun et al. 2005)). Cependant, si ces abstractions simplifient les règles, écrire une règle comprenant des abstractions est plus complexe nécessitant une phase d'analyse. Par exemple, assigner une permission à un rôle dans une hiérarchie de rôles nécessite de comprendre que cette permission sera propagée aux rôles supérieurs. D'un autre côté, ne pas utiliser d'abstraction n'est pas une solution non plus car cette approche ne passe pas le facteur d'échelle comme cela a été prouvé dans le contexte de la gestion de la sécurité des réseaux d'entreprises. Nous avons essayé de proposer un système qui recommande aux particuliers des règles de sécurité utilisant des abstractions. Ce dernier axe de recherche est résumé dans le chapitre 6.

[2] http://www.frost.com/prod/servlet/press-release.pag?docid=291568194

Enfin je termine ce manuscrit par une conclusion ainsi que différentes perspectives de recherche sur des problématiques qui me semblent importantes à traiter dans le futur.

Chapitre 2. Gestion des identités et des accès dans les infrastructures virtuelles

Ces travaux ont été traités dans le cadre des thèses de Michel Kamel (Kamel 2008) et de Bashar Kabbani (Kabbani 2015).

2.1 Présentation de la problématique

La gestion des identités et des accès (Identity & Access Management - IAM) est aujourd'hui considérée comme un projet à part entière dans les entreprises. Entre respect des obligations réglementaires et optimisation de l'administration des droits, les projets IAM renforcent le niveau de sécurité général tant sur les plans fonctionnel (ressources humaines) que technique. La multiplicité des applications métiers nécessitant chacune un contrôle d'accès propre et une administration des droits spécifiques a favorisé les exigences d'une vision globale et l'émergence de processus de gestion des accréditations bien identifiés. La séparation claire des préoccupations et des problèmes de responsabilité a conduit à adopter un modèle organisationnel faisant apparaître différentes entités : fournisseur de service (SP), fournisseur d'identité (IdP), demandeur, et plate-forme de gestion des identités.

Le fournisseur de service constitue le cœur de l'application métier. Lorsqu'un utilisateur sollicite un service particulier, il en fait la demande. Il doit pour cela se réclamer d'une identité dont la vérification exige la mise en place d'un service d'authentification. Cette vérification peut être réalisée systématiquement lors de chaque demande effectuée par l'application métier. Ainsi un utilisateur peut disposer de plusieurs identités au sein du même système d'information, ouvert ou non, et différentes solutions d'authentification peuvent coexister. Des technologies d'authentification unique (Single Sign-On) ont vu le jour permettant de limiter les interactions avec l'utilisateur fondées sur une relation de confiance entre les différents partenaires (IdP et SP). Des protocoles comme OpenID ou OAuth ont été conçus pour permettre à des plates-formes Web de déléguer la gestion de l'authentification en ligne : ils permettent de récupérer des éléments d'authentification auprès d'un fournisseur d'identité. La plupart des plates-formes des réseaux sociaux – Facebook ou Twitter en particulier – y font appel.

Le concept de fédération d'identité puise également sa source dans les besoins de rationalisation des informations d'identité, d'interopérabilité et d'ouverture des systèmes d'information aux partenaires. On parle alors d'identité fédérée qui apporte des avantages fonctionnels aussi bien pour l'utilisateur que pour l'entreprise (Morgan et al. 2004). Le bénéfice pour les IdP chargés d'authentifier l'utilisateur et de gérer son identité, est de proposer un large éventail de services sans coût additionnel.

Dans le même temps, un service d'autorisation pertinent est indispensable pour éviter aux SPs une perte de contrôle qui aboutirait à laisser des utilisateurs d'autres domaines entrer dans leurs systèmes d'information (Kamel 2008; Landau et al. 2012).

La gestion des accès complète la gestion des identités dans l'offre de sécurité. « Qui peut faire quoi, où, et quand ? » sont les questions que se posent désormais les administrateurs pour lesquels la protection des données personnelles et partagées est une exigence de plus en plus forte. Chaque ressource, fournie par une organisation, doit être protégée par des règles qui la rendent accessible aux seules entités ayant les accréditations nécessaires et dans les conditions déterminées. L'écriture de telles règles devient complexe lorsque les ressources sont partagées entre plusieurs organisations et que les utilisateurs proviennent de différentes organisations. De plus, les règles d'accès doivent prendre en compte la dynamique des systèmes gérés. Selon l'état du système, différentes règles doivent être effectives. Nous avons essayé de proposer des solutions à ces différentes questions.

Dans ce chapitre, je commence par introduire l'évolution des besoins de gestion de la sécurité à travers l'évolution des infrastructures et des besoins de collaborations. Ensuite, je présenterai les approches de gestion des identités et les modèles de déploiements. Après je m'attarderai sur la gestion des accès en traitant à la fois l'expression de politique que les architectures de déploiement. Cela me permettra de exposer quelques travaux que nous avons menés dans le domaine de la gestion des identités et des accès.

2.2 De l'infrastructure physique à l'infrastructure virtuelle

Lorsque j'ai commencé dans le monde de la recherche en 2000/2001, les réseaux d'entreprises étendues se tissaient, brisant le concept de l'entreprise intégrée (Mariotti et al. 2001). Dans le modèle de l'entreprise intégrée, une société réalise en interne la totalité des étapes nécessaires à son activité (conception, production, distribution, etc.) maîtrisant ainsi la totalité de la chaîne de valeur (Baglin et al. 2002). Contrairement à l'entreprise intégrée, dans l'approche de l'entreprise étendue, une société dite maître d'œuvre se recentre sur son cœur de métier et externalise certaines tâches à d'autres entreprises de type sous-traitants, fournisseurs, prestataires, etc., et cela sans les accueillir dans ses locaux. L'infrastructure réseau de ce nouveau modèle d'entreprise devait donc prendre en compte cet éclatement. Il était alors devenu nécessaire d'interconnecter les réseaux privés des entreprises entre eux. L'approche de mettre en œuvre une ligne spécialisée qui permet de construire un réseau privé global à toute l'entreprise étendue était coûteuse et peu flexible. Or l'avènement du réseau Internet permettait d'utiliser ce réseau comme dorsale de communication pour interconnecter les réseaux des membres de l'entreprise étendue. Ajouté à cela, cette interconnexion nécessitait d'ouvrir les réseaux privés et il était donc nécessaire de contrôler cette ouverture des réseaux en particulier celui de l'entreprise maître d'ouvrage. Les contours du réseau de l'entreprise n'étant plus limités au réseau privé uniquement, une simple démarcation réseau privé (réseau sûr) versus réseau publique (réseau non sûr) n'était plus adaptée. Il était indispensable de définir des zones de cloisonnement à l'intérieur

du réseau privé des entreprises et de les interconnecter au travers de tunnels sécurisés afin de créer des réseaux privés virtuels (Barrere et al. 2002).

Par la suite, la notion d'entreprise étendue a évolué vers les concepts d'entreprise virtuelle puis d'organisation virtuelle. Une organisation virtuelle prend naissance lorsque plusieurs organisations se réunissent pour réaliser communément un projet ou une activité économique, et où chaque organisation se concentre sur ce qu'elle sait faire de mieux, en s'appuyant sur le savoir-faire des autres et en échangeant des informations par le biais des technologies d'information (TI) (Meissonier 2000). Le concept d'organisation virtuelle ne correspond pas uniquement à un besoin d'externalisation mais à une réelle collaboration entre entreprises. Ces nouveaux usages ont amené de nouvelles contraintes en terme de gestion de la sécurité. Contrairement à l'entreprise étendue qui a une durée de vie longue (Browne et al. 1999), l'existence de l'organisation virtuelle est de nature temporaire et sa durée de vie est rattachée au but recherché lors de sa mise en place. La dynamicité de l'infrastructure virtuelle - support de l'organisation virtuelle - s'en est trouvée accrue. Les contours de ces infrastructures sont plus malléables et mouvantes. Ajouté à cela, il n'y a pas forcément de hiérarchie où une entreprise est maître d'œuvre et les autres sous-traitants, etc. Par conséquent, une gestion centralisée n'est plus adaptée. Plusieurs acteurs provenant d'organisations différentes interviennent alors dans la chaîne de gestion[3] de la sécurité de l'organisation virtuelle. En effet, chaque partenaire doit être capable de gérer les ressources qu'il propose à l'organisation virtuelle tant en terme de ressources humaines que TI. Enfin, l'organisation virtuelle offre plus de flexibilité. En effet, il est possible de créer des équipes virtuelles, mutualisant les ressources humaines de chaque partenaire, qui utilisent des ressources TI elles-mêmes virtuelles et mutualisées. La gestion de la sécurité d'un tel environnement ne peut plus se limiter à la mise en œuvre de configurations sur les équipements de sécurité réseau des partenaires. Gérer les accès des utilisateurs sur les ressources est alors nécessaire.

Aujourd'hui, la virtualisation des infrastructures s'est encore amplifiée avec le développement des technologies de virtualisation offrant la possibilité d'avoir des machines virtuelles, des équipements réseaux virtuels, des systèmes d'information virtuels, etc. Le niveau de maturité atteint par ces technologies de virtualisation combiné avec la puissance disponible de calcul du matériel et les débits proposés par les réseaux permettent de proposer de l'informatique virtuelle comme on propose un service. Percevoir l'informatique comme un service a été formalisé dans le cadre du standard ITIL puis de la norme ISO 20000. Cependant, le terme qui médiatise actuellement ce concept est « l'informatique en nuage » (ou plutôt « cloud computing » pour être à la mode). Que l'on considère ce terme comme une révolution[4] dans le domaine informatique ou uniquement marketing[5], une

[3] Par chaîne de gestion de la sécurité, je veux exprimer les différents acteurs devant interagir dans la définition et la mise œuvre d'une politique de sécurité globale.

[4] Point de vue de FORBES : http://www.forbes.com/sites/truebridge/2013/09/25/software-revolution-part-ii-the-shift-to-cloud-computing/

[5] Point de vue de R. Stallman : http://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman

entreprise peut aujourd'hui louer une application, une partie de son infrastructure informatique, voire presque la totalité de son infrastructure (auquel cas le matériel physique nécessaire se limite à un terminal connecté à Internet) à un fournisseur de service informatique. Le niveau de flexibilité offert par cette approche orientée service rend les contours de l'infrastructure virtuelle toujours plus flous et plus dynamiques. Ajouté à cela, selon le niveau de service défini dans son contrat signé avec le fournisseur de service informatique, l'entreprise peut aussi déléguer selon ses besoins la gestion de cette infrastructure virtuelle au fournisseur ou alors garder le contrôle. La chaîne de gestion est alors rendue encore plus complexe.

Ainsi, les infrastructures informatiques en devenant virtuelles permettent de nouveaux usages, limitent les coûts d'achats, offrent plus de flexibilité permettant aux entreprises de mieux réagir et évoluer. Par conséquent, la gestion de la sécurité de ces infrastructures doit prendre en compte cette dynamicité : leurs frontières sont floues et malléables, les besoins des utilisateurs de ces infrastructures sont multiples et la gestion de ces environnements est collaborative.

2.3 Gestion des identités

Une identité est une représentation d'une entité dans un domaine d'application spécifique. Une identité permet de singulariser, nommer, isoler une entité prise parmi un ensemble. A priori, on attend d'une identité, qu'elle soit associée à une entité unique. Il ne faut pas la confondre avec une identité commune, qui est associée à des entités élémentaires ayant une relation de groupe. Ainsi, dans une famille, l'identité commune est donnée par le nom de famille, qui devient alors une caractéristique appartenant aux différents membres du groupe. Dans la mesure où le fournisseur de services est concerné, ce dernier peut traiter l'entité commune (la famille) et non pas un ensemble d'individus. Une entité peut avoir des identités multiples, certaines pouvant être des synonymes. Suivant le contexte, une entité peut ainsi avoir de 1 à *n* identités. Les règles d'enregistrement des identités dans un domaine spécifique déterminent si une entité a le droit d'avoir plusieurs identités dans ce domaine spécifique. Une personne peut toujours avoir plusieurs identités dans des domaines différents. Par exemple, une personne peut avoir une identité associée en tant qu'utilisateur d'un service de courriel et une autre identité associée en tant qu'employé d'une université. Une identité est construite à partir d'un ensemble d'attributs représentant des caractéristiques (ISO 24760 2011)

Ces caractéristiques peuvent avoir diverses propriétés telles qu'être temporaires ou permanentes, auto choisies par l'entité ou bien affectées par une autorité, avoir une portée limitée à une organisation, ou bien dépasser les limites de cette même organisation.

Selon la norme ISO/IEC 24760 (ISO 24760 2011), la gestion des identités inclut la gouvernance, les politiques, les processus, les données, les technologies et les standards permettant entre autre :

- d'authentifier les identités,
- d'établir la provenance des informations des identités,
- d'établir le lien entre les informations sur les identités et les entités,
- de maintenir à jour les informations sur les identités,
- d'assurer l'intégrité des informations sur les identités,
- de fournir les justificatifs d'identité et les services pour faciliter l'authentification d'une entité en tant qu'identité reconnue,
- d'ajuster les risques de sécurité liés au vol d'information par exemple.

Pour cela, l'ISO préconise de gérer les identités selon le cycle de vie décrit dans la Figure 3. Plusieurs technologies sont utilisées de nos jours pour gérer les identités dans un domaine de sécurité ou au moins, permettre aux administrateurs TI des organisations de contrôler les identités des utilisateurs internes et externes. Nous entendons par gérer une identité le fait de vérifier l'identité d'une entité à travers des moyens physiques (par exemple, rencontre de l'entité en question), attribuer à cette entité les accréditations (identificateurs et caractéristiques uniques) et enfin l'authentifier chaque fois qu'elle désire accéder à un service protégé.

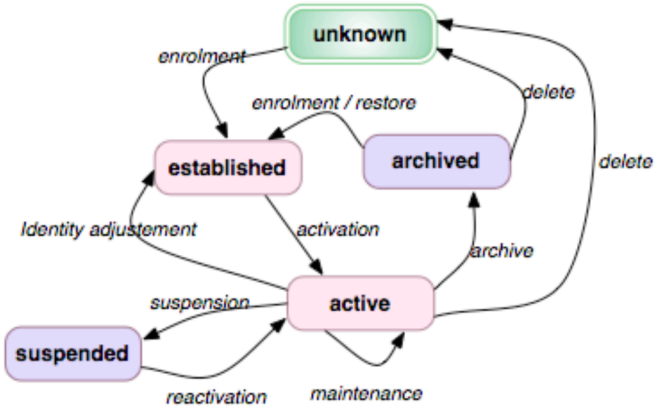


Figure 3. Cycle de vie des identités (ISO 24760 2011)

Il existe plusieurs modèles de gestion des identités. Jøsang et al. (Jøsang et al. 2005) en ont défini trois : le modèle isolé, le modèle commun et le modèle d'authentification unique. Dans le *modèle isolé,* chaque fournisseur de service gère les identités des utilisateurs. Donc l'utilisateur possède *x* comptes différents pour accéder à *x* services. Le *modèle commun* indique qu'un seul fournisseur d'identificateurs et d'attributs est utilisé par plusieurs fournisseurs de services pour gérer les comptes de leurs utilisateurs. Dans ce cas de figure, une seule autorité endosse les responsabilités d'identifier, d'affecter et de valider l'identité des utilisateurs communiquant avec l'ensemble des fournisseurs de services. Par contre, l'utilisateur doit se connecter (avec les mêmes informations) à chaque service. Enfin, le *modèle d'authentification unique* étend le modèle commun où l'utilisateur ne s'authentifie qu'une seule fois. Son identité est alors propagée aux différents services.

Les besoins de partage des identités entre différents domaines de gestion ont donné lieu au concept de fédération d'identité. La fédération d'identité (CLUSIF 2007) ou authentification répartie est un partage d'informations d'identité concernant les utilisateurs d'un établissement, avec une organisation partenaire qui vise à permettre l'accès à distance contrôlé et sécurisé aux ressources de ce partenaire. La fédération concrétise, pour un groupement d'organisations, l'interconnexion de leurs services d'authentification et l'utilisation d'un ensemble commun d'attributs utilisateurs. Un établissement qui gère un ensemble d'utilisateurs (identificateurs et attributs) est appelé fournisseur d'identités (*IdP : Identity Provider*). Un fournisseur de services (*SP*) est une entité (e.g. établissement, administration, entreprise, etc.) qui propose une ressource numérique en ligne au sein de la fédération. Etablir une fédération d'identité entre organisations revient à définir un cercle de confiance entre des fournisseurs d'identité et des fournisseurs de services de sorte que ces derniers acceptent des accréditations émises par les fournisseurs d'identité pour leurs propres utilisateurs.

Une même organisation peut participer à plusieurs fédérations et gérer des partenariats de manière bilatérale. Elle peut également jouer à la fois le rôle de fournisseur d'identités et de fournisseur de services. La fédération d'identité est fondée sur deux concepts :

1) la délégation de l'authentification qui consiste à authentifier l'utilisateur depuis le service d'authentification interne (organisation mère de l'utilisateur), et non pas depuis celui du fournisseur de l'application (fournisseur de service)
2) la propagation des attributs utilisateurs qui permet de prolonger depuis l'organisation mère de l'utilisateur l'exploitation d'un identifiant unique et des attributs de comptes internes afin de communiquer avec le fournisseur de services.

Afin de préserver la sécurité de l'information, des métadonnées liées à l'identité doivent être échangées entre les organisations (fournisseurs d'identité et fournisseurs de services). Ces informations incluent la preuve de l'authentification de l'utilisateur auprès de son organisation de rattachement, la méthode d'authentification utilisée, la date et l'heure de l'authentification, etc. Ceci, permet aux fournisseurs de services d'appliquer des politiques de sécurité dépendamment du contexte d'authentification de l'utilisateur. Plusieurs langages ont été développés dans ce sens tels que SAML (OASIS SAML 2015) ou WS-Federation (Bajaj et al. 2003).

Le modèle commun de gestion des identités peut correspondre aux besoins de l'entreprise étendue. En effet, l'entreprise maître d'œuvre peut gérer les identités des employés des entreprises annexes de par sa position centrale. Toutefois, cela lui demande de mettre en œuvre des procédures supplémentaires qui peuvent être complexes et coûteuses dans le cas d'un nombre important de participants. Par contre, ce modèle de gestion ne peut convenir aux interactions de type organisation virtuelle où il n'existe pas de hiérarchie naturelle entre organisations.

La notion de fédération d'identités permet à chaque entreprise de gérer les identités de ses employés. Il faut alors standardiser des attributs afin de définir un référentiel commun à la fédération.

La gestion des identités d'une structure virtuelle est alors simplifiée car elle s'intègre dans la gestion des identités de chaque entreprise. Ainsi, si un employé ne travaille plus pour une entreprise, cette entreprise peut en supprimant l'identité de l'employé supprimer les identités liées aux structures virtuelles. Cependant, la fédération d'identité impose de faire confiance aux fournisseurs d'identités car cette activité est externalisée du point de vue de celui qui offre les ressources. L'adoption du principe de fédération d'identité a aussi un autre intérêt. La fédération ne fait qu'utiliser les moyens d'authentification, d'autorisation et de sécurisation implémentés par les organisations partenaires ce qui favorise un déploiement rapide et à faible coût du réseau collaboratif en évitant un blocage qui pourrait naître de l'absence d'un mécanisme commun d'authentification.

2.4 Gestion des accès

Selon le RFC 2904 de l'IETF (Vollbrecht et al. 2000), les entités de base qui participent à une autorisation sont (Figure 4) :

- un utilisateur qui demande un service,
- l'organisation mère de l'utilisateur partie prenante au contrat établi et qui doit vérifier sous une forme active ou passive si l'utilisateur est habilité ou non à déclencher l'exécution du service,
- le serveur AAA du fournisseur de services qui autorise l'accès au service en se basant sur le contrat signé avec l'organisation mère de l'utilisateur,
- l'équipement de service dédié à la fourniture de services en réponse aux demandes de service.

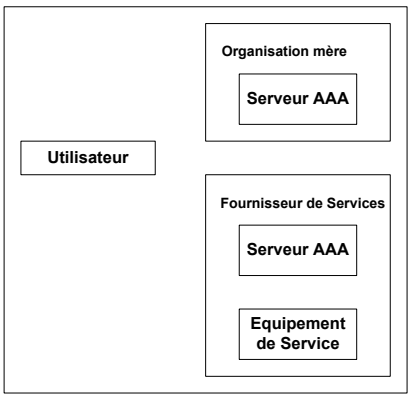


Figure 4. Architecture d'autorisation AAA (Vollbrecht et al. 2000)

Nous nous sommes intéressés aux architectures mettant en œuvre la fonction d'autorisation par le biais du concept de politiques de contrôle d'accès (PBMS : Policy Based Management Systems).

2.4.1 Architectures de gestion des autorisations

Les systèmes de gestion à base de politiques sont une solution de remplacement des listes de contrôle d'accès ou ACLs[6] intégrées habituellement aux applications gérées qui rend la gestion plus dynamique et évolutive. Avec une telle approche, deux actions de gestions sont distinguées : i) les décisions d'autorisation prises après consultation des politiques, et ii) l'application de ces décisions sur le système géré. Ces deux fonctions sont accomplies par deux entités distinctes nommées respectivement PDP (Policy Decision Point) et PEP (Policy Enforcement Point).

- Un PDP est une entité logique qui prend des décisions d'autorisation en considérant les informations suivantes (RFC 2906) :
  - la ressource demandée et l'action requise (consultation, modification, etc.) ;
  - l'entité qui demande la ressource ;
  - la politique qui gère l'accès à la ressource.
- Un PEP est une entité logique qui applique la décision d'autorisation prise par le PDP. C'est le PEP, gardien de la ressource, qui réalise techniquement l'accès. Les interactions entre PDP et PEP peuvent suivre l'un des trois modèles suivants : Agent, Push ou Pull.

2.4.1.1 Le Modèle Agent

Le modèle agent permet à l'utilisateur d'adresser sa requête de demande de ressource à une partie tierce (le serveur d'autorisation : PDP/PEP). Ce dernier joue le rôle d'agent entre l'utilisateur et l'équipement fournissant le service. Le serveur d'autorisation applique la politique associée à cette demande. Si l'accès est autorisé, le serveur transfère la requête de l'utilisateur à la ressource ; sinon, il renvoie un message d'interdiction à l'utilisateur. La ressource retourne le résultat de la requête au PEP qui à son tour le transfère à l'utilisateur. Dans ce cas là, le PEP se trouve au niveau du serveur d'autorisation (**Figure 5**).

2.4.1.2 Le Modèle Push

L'utilisateur adresse sa requête directement au fournisseur de service (i.e. la ressource demandée) et en particulier, au serveur d'autorisation (PDP) qui gère l'accès à la ressource. Ce dernier définit l'information d'autorisation (le droit d'accès ou pas à la ressource) qui est renvoyée à l'utilisateur sous forme d'un ticket. L'utilisateur présente le ticket acquis avec la demande d'accès à la ressource. Ainsi, le PEP qui se trouve au niveau de la ressource cette fois-ci donne le droit d'accès à l'utilisateur si le ticket est valide (**Figure 6**).

[6] Access Control List

2.4.1.3 Le Modèle Pull

Le modèle pull laisse la responsabilité de la récupération de l'information d'autorisation au PDP seul. Une fois que l'utilisateur a demandé l'accès à une ressource, le PEP qui se trouve au niveau de cette dernière, récupère l'information d'autorisation d'une façon active auprès du PDP et donne le droit d'accès à l'utilisateur si la décision est affirmative (Figure 7).

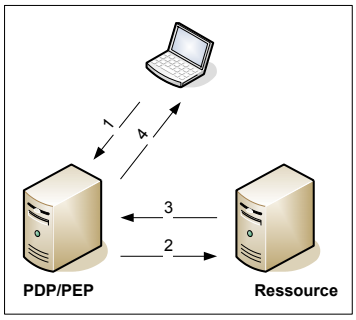


Figure 5. Modèle agent

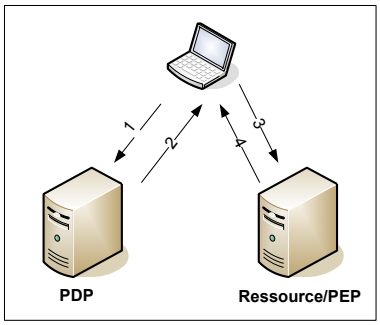


Figure 6. Modèle push

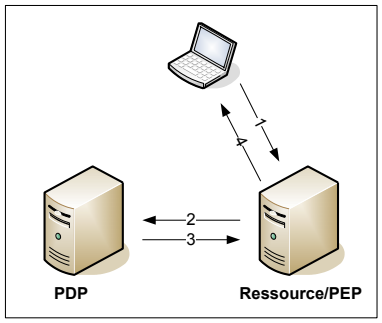


Figure 7. Modèle pull

Le modèle Agent convient mieux dans le cas de fédération d'organisations membres s'appuyant sur une entité tierce pour la gestion des accès aux ressources partagées comme dans le cas d'une entreprise étendue avec une autorité centrale.

Les modèles Push et Pull sont également adaptés aux organisations virtuelles où chacun des membres garde le contrôle sur ses propres ressources et à qui il revient d'autoriser les utilisateurs d'un partenaire d'accéder les ressources partagées. Préférer un modèle à un autre est une question de choix stratégique et n'a rien à voir avec la performance ou la capacité des modèles.

2.4.2 Modèles de contrôle d'accès

Les politiques de contrôle d'accès sont des représentations d'exigences spécifiant comment les accès sont gérés et qui, dans quelles circonstances, peut accéder à quelle information. Afin d'exprimer des politiques de contrôle d'accès qui soient cohérentes et empêcher des brèches de sécurité dans les systèmes protégés, des modèles de contrôle d'accès sont utilisés pour l'expression de ces politiques. Ces modèles permettent une représentation formelle des politiques.

Bien qu'il existe de nombreux modèles ayant chacun leurs caractéristiques, il y a une base commune. Tous ces modèles considèrent trois ensembles :

- **l'ensemble des objets O** représentant les ressources ou les services à contrôler,
- **l'ensemble des sujets S** représentant les entités qui veulent exécuter des actions sur les objets. Ces entités peuvent représenter des utilisateurs ou des applications,
- **l'ensemble des droits d'accès R** représentant comment les sujets peuvent accéder aux ressources.

Les modèles proposés dans les années 70 et 80 avaient la volonté de prouver qu'une politique exprimée garantissait une propriété de sécurité. L'une des premières modélisations d'une politique

introduite par Lampson (Lampson 1974) se limitait à une simple matrice représentée par une fonction $S \times O \rightarrow 2^R$. Dans cette famille de modèles que l'on nomme modèles discrétionnaires (Discretionary Access Control ou DAC), chaque sujet est administrateur de ses ressources ; le fait de posséder un objet permet de modifier les droits d'accès sur celui-ci. Les chercheurs se sont alors posés le problème de protection (safety problem) : Existe-t-il une séquence d'opérations qui amène un droit d'accès α à se retrouver dans une case de la matrice d'accès où il ne devrait pas être ? Des approches telles que le modèle HRU (Harrison et al. 1976), Take-Grant (Jones et al. 1976) ou de protection schématique (Sandhu 1988) ont essayé d'établir la décidabilité de ce problème en restreignant la capacité de modification de la matrice. Mais il a été démontré que le problème est indécidable dans le cas général. Il n'est décidable qu'avec de fortes restrictions mais avec une complexité polynomiale par rapport à la taille de la matrice voire NP-complet. En parallèle, des modèles ont supprimé le droit de possession et ont proposé des métarègles que toute politique doit satisfaire pour garantir une certaine propriété de sécurité. Cette famille de modèles est nommé modèles obligatoires (Mandatory Access Control ou MAC). Par exemple, le modèle de Bell-Lapadula (Bell et al. 1973) a été défini au moment où les militaires désiraient louer leur mainframe à des entreprises. La problématique était alors de contrôler le flux d'information afin de prévenir des fuites d'informations sensibles (Bell 2005). Tout d'abord, ils ont ajouté des métadonnées sur les sujets et les objets appelées respectivement niveau d'habilitation et de classification. Des métarègles, appelées conditions de simple sécurité, propriété étoile et propriété de sécurité discrétionnaire, garantissent qu'une information sensible ne peut pas être lue par un sujet n'ayant pas le niveau d'habilitation suffisant. Une approche similaire a été suivie par Biba (Biba 1977) pour garantir la propriété d'intégrité.

Dans les années 90, l'ordinateur pénètre dans tous les milieux sociaux, et dans tous les systèmes technique, financier, commercial, d'information, administratif[7]. Un problème de gestion se pose alors : comment gérer efficacement les droits de tous ces utilisateurs. Le modèle Role Based Access Control (RBAC) (Ferraiolo et al. 1995; Ferraiolo et al. 2003) s'est imposé en préconisant de gérer les permissions des utilisateurs par rapport à leur fonction (rôle) plutôt que par rapport à leur identifiant. On voit alors que les efforts de recherche dans ce domaine ne portent plus sur la preuve qu'une politique est « bonne » mais sur comment rajouter des métadonnées pour simplifier les politiques en exprimant de plus en plus de contraintes qui dépendent des problématiques du moment. Ainsi les besoins de collaboration des années fin 90/début 2000 ont amené des modèles comme TMAC (TeaM based Access Control) (Thomas 1997) ou OrBAC (Organization Based Access Control) (Kalam et al. 2003). Depuis le milieu des années 2000, on voit apparaître des modèles qui introduisent la notion de contexte correspondant aux besoins de l'informatique pervasive/ubiquitaire comme LRBAC (Location Based Access Control) (Zhang et al. 2006), GTRBAC (Generalized Temporal RBAC) (Joshi et al. 2005), CRBAC (Context RBAC) (Park et al. 2006), Context dans OrBAC (Cuppens et al. 2003). Cette

[7] wikipedia : https://fr.wikipedia.org/wiki/Histoire_de_l%27informatique#L.27explosion_:_de_1990_.C3.A0_nos_jours

période s'est aussi attachée aux problématiques liées à la protection de la vie privée. Nous pouvons voir émerger des modèles proposant des concepts comme les intentions (Byun et al. 2005), la confiance (Wagealla et al. 2003), la précision des informations données ou le consentement (Ajam et al. 2010). En parallèle, l'émergence de l'informatique en nuage a remis au goût du jour les modèles initialement créés pour les mainframes comme Bell-Lapadula (Watson 2012).

De mon point de vue, les modèles de contrôle d'accès après les années 90 sont des patrons de conception de politique. En effet, ils proposent des solutions qui répondent à des problèmes récurrents comme les patrons de conception qui existent dans le domaine du génie logiciel. Au travers de métadonnées à associer aux identités des sujets et des objets, ils simplifient les politiques de sécurité pour exprimer des contraintes répondant à des besoins types (e.g., la collaboration, la contextualisation, la vie privée, etc.)

Ne voulant pas proposer des solutions de gestion limitées à un problème donné, je me suis tourné dès 2007 vers une autre démarche appelée Attribute Based Access Control (ABAC) (NIST ABAC 2015). ABAC n'est pas un modèle de politique mais un modèle pour exprimer des politiques. Dans l'approche ABAC, tout élément significatif en terme sécurité peut être considéré comme un attribut. Par exemple, le rôle d'un utilisateur est un attribut, la position GPS d'une ressource est un attribut, le paramètre d'une méthode exécutée sur une ressource est un attribut, etc. Une politique de sécurité devient alors une expression sur un ensemble d'attributs.

Ainsi, l'intégration entre gestion des identités et des accès est naturelle ; la gestion des identités modélisant les identités en terme d'attributs et la gestion des accès définissant les politiques aussi en terme d'attributs. Ces attributs pouvant provenir de modèles de contrôle d'accès selon le contexte de sécurisation considéré.

Partant de ce constat, nous avons travaillé sur le standard international qui met en œuvre la démarche ABAC : eXtensible Access control Markup Language (OASIS XACML 2015).

2.4.3 Le standard XACML

Le standard XACML est une spécification XML édictée par l'OASIS[8] pour la définition de politiques de contrôle d'accès. XACML v3 (OASIS XACMLv3 2013) fournit un langage de description des politiques de contrôle d'accès et une architecture pour la mise en œuvre du contrôle d'accès par un protocole de type requête/réponse donnant les moyens d'exprimer des requêtes d'accès et les réponses appropriées. L'un des avantages de XACML est de favoriser l'interopérabilité entre les produits d'administration et d'autorisation hétérogènes présents sur le marché.

La politique de contrôle d'accès permet de définir les droits des utilisateurs (personne ou application) sur les ressources informatiques (données, services, etc.). XACML est un langage d'expression puissant qui utilise la logique pour combiner les règles où toute information de sécurité

[8] Organization for the Advancement of Structured Information Standards

est considérée comme un attribut du sujet, de la ressource, de l'action ou de tout autre objet de sécurité (XACML appelle cela des catégories).

L'architecture XACML est représentée ci-dessous (Figure 8) et opère selon les étapes suivantes :

- Le *Policy Administration Point* (PAP) écrit les politiques et les rend disponibles au PDP. Ces politiques représentent la politique complète qui contrôle les décisions prises par le PDP.
- Le demandeur d'accès envoie une requête d'accès au PEP.
- Le PEP envoie la requête d'accès au *context handler* au format natif (langage supporté par le PEP), optionnellement incluant des attributs pour le sujet, la ressource et l'environnement.
- Le *context handler* construit un contexte de requête XACML et l'envoie au PDP.
- Le PDP peut demander des attributs additionnels pour le sujet, la ressource et l'environnement du *context handler*.
- Le context handler demande ces attributs du Policy Information Point (PIP).
- Le PIP obtient les attributs demandés qui peuvent être stockés dans différentes bases de données, annuaires, etc.
- Le PIP retourne les attributs demandés au *context handler*.
- Le *context handler* envoie les attributs demandés au PDP qui évalue la politique.
- Le PDP retourne le contexte de réponse XACML (incluant la décision d'autorisation) au *context handler*.
- Le *context handler* traduit le contexte de réponse XACML au format de réponse natif du PEP. Le *context handler* retourne la réponse au PEP qui applique la décision d'autorisation.
- Lorsque la décision inclut des obligations (par exemple, « si la décision est « permit » alors envoyer un courriel à l'administrateur »), le PEP met alors en œuvre ces obligations via un service dédié.

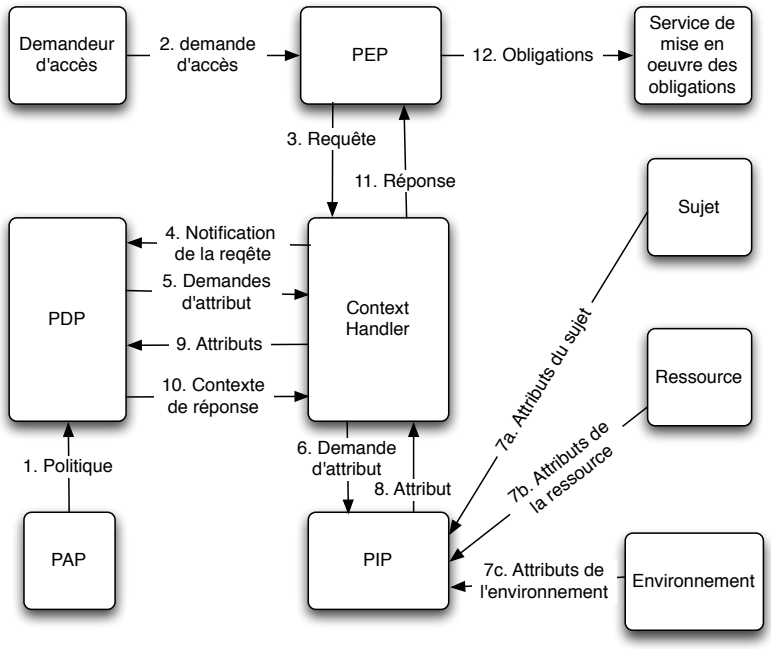


Figure 8. Architecture XACML

XACML est adapté aux environnements distribués où les PEPs et PDPs sont répartis au niveau d'infrastructures hétérogènes. En séparant les politiques d'accès des applications protégées et en proposant un standard pour l'expression des autorisations, XACML permet aux systèmes de sécurité hétérogènes de partager les politiques. Ainsi, les administrateurs de systèmes ne sont plus obligés d'écrire leurs politiques en utilisant différents langages.

Une politique XACML est composée d'une cible *Target*, d'un ensemble de règles *Rules* et d'un ensemble facultatif d'éléments d'*Obligations* et d'*avis* qui s'appliquent à la requête (Figure 9). L'élément *Target* permet d'identifier la politique ou les règles applicables à une requête d'accès ; il spécifie les conditions que le sujet, la ressource et l'action doivent vérifier afin qu'une politique ou une règle soit applicable à la ressource requise. Ainsi, l'élément *Target* fournit un moyen d'indexation et de recherche de politiques. Une fois que la politique applicable est identifiée, les règles sont évaluées.

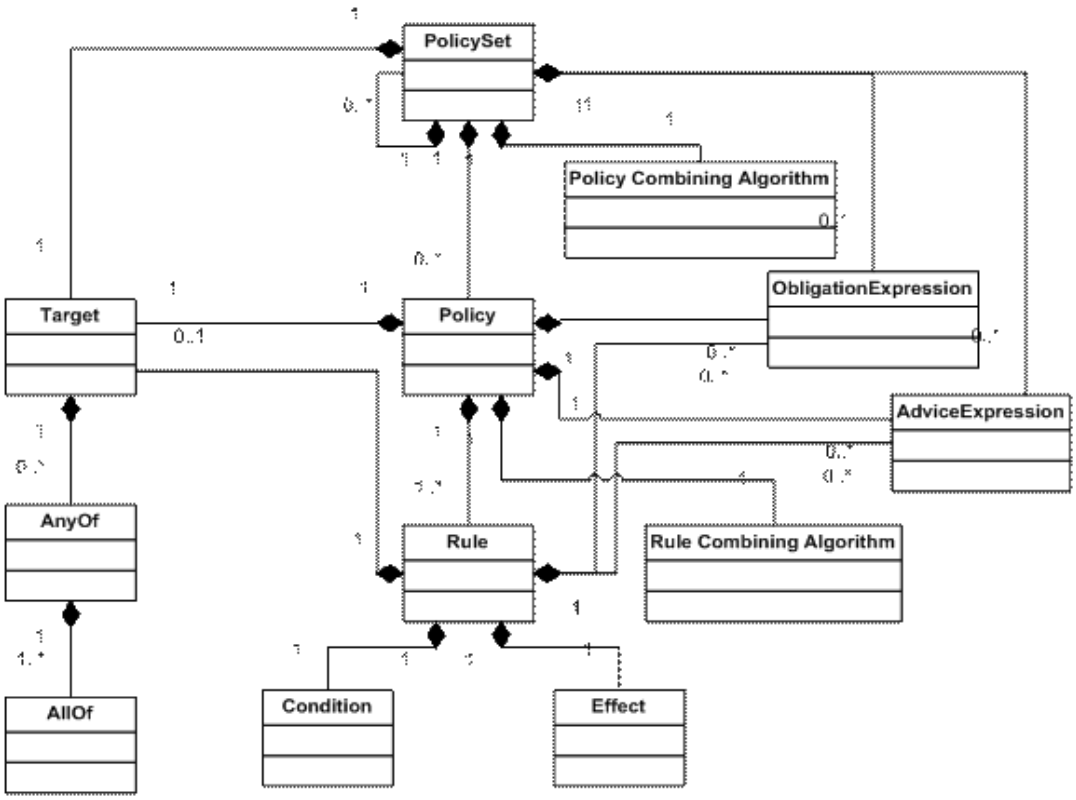


Figure 9. Modèle du langage de politique XACMLv3

XACML fournit le moyen d'exprimer des « obligations » ainsi que des « avis » au niveau des règles à considérer par un PEP. On peut noter aussi que la puissance de XACML provient de son caractère extensible par l'ajout 1) de nouveaux attributs (sujet, action, ressource ou environnement), 2) de nouvelles fonctions pour manipuler les attributs, 3) ou encore de nouveaux algorithmes de combinaison permettant d'arrêter une décision tant au niveau des règles que des politiques. L'étude de l'extensibilité de XACML ayant donné un axe complet de recherche. Il sera traité de manière détaillée dans le chapitre suivant.

2.5 Gestion des accès et des identités dans les organisations virtuelles

Dans le cadre du projet européen VIVACE, nous avons travaillé sur la gestion des identités et des accès lors de la construction d'organisations virtuelles dans le monde aéronautique. Nous avons traité ce problème sous les deux angles : technique et organisationnel. Dans (Laborde, Kamel, et al. 2009), nous avons traité le problème d'un point de vue technique en montrant que l'association des fédérations d'identités et la gestion des autorisations avec des attributs répond aux besoins des organisations virtuelles. En effet, la fédération d'identité permet à chaque organisation de gérer les identités de ses employés. Ainsi, il est possible de donner à chaque organisation la capacité d'assigner des valeurs d'attributs aux identités utilisées dans l'organisation virtuelle ; ce que l'on appelle *autorité d'attribut* dans les Infrastructures de Gestion des Permissions (Chadwick et al. 2003). Par exemple dans la Figure 10, l'entreprise A a autorité pour assigner le rôle Analyzer, l'entreprise B le rôle

Designer, etc. L'émetteur de la valeur de l'attribut rôle est alors pris en compte dans les règles d'autorisation grâce à la flexibilité de l'approche ABAC. L'approche ABAC permet aussi de prendre en compte le dynamisme des permissions. Dans l'exemple de la Figure 10, un « conductor » définit un workflow où dans la phase *Design* seules les personnes avec le rôle *Designer* pouvent accéder à une donnée, puis vient la phase *d'analyse* où seules les personnes avec le rôle *Analyzer* peuvent accéder la donnée, etc. La première idée avait été que le « conductor » puisse ajouter et supprimer des règles afin de mettre en œuvre les permissions dynamiques. Par exemple, lorsque la phase d'analyse commence, enlever la règle « si role = designer alors permit » et ajouter la règle « si role = analyzer alors permit ». Or cela donne un pouvoir d'administration au « conductor ». L'approche ABAC permet d'éviter cela en introduisant un attribut représentant la phase du workflow où ce n'est pas la politique qui est dynamique mais uniquement les permissions. La politique prend alors la forme suivante : si phase = design et role = designer alors permit, si phase = analysis et role = analyzer alors permit, etc. L'autre avantage est que le « conductor » n'est plus administrateur de la politique mais simplement une autorité pour l'attribut *phase*, ce qui correspond mieux à sa fonction d'origine. Ceci montre l'intérêt de l'approche ABAC. Enfin, nous avions démontré qu'il était possible de coupler une fédération d'identité (dans notre cas Shibboleth) et un système d'autorisation ABAC (ici XACML) au travers d'un prototype (Figure 11).

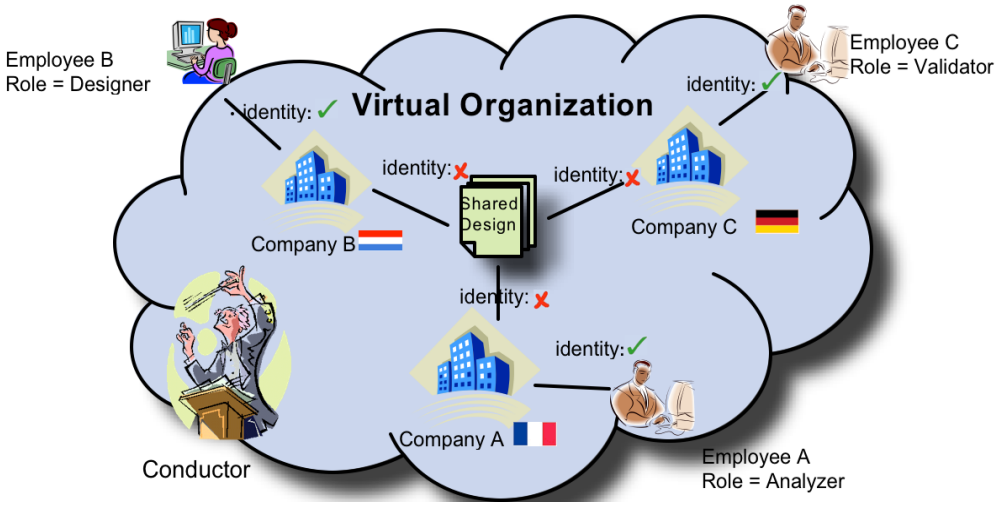


Figure 10. Exemple d'organisation virtuelle

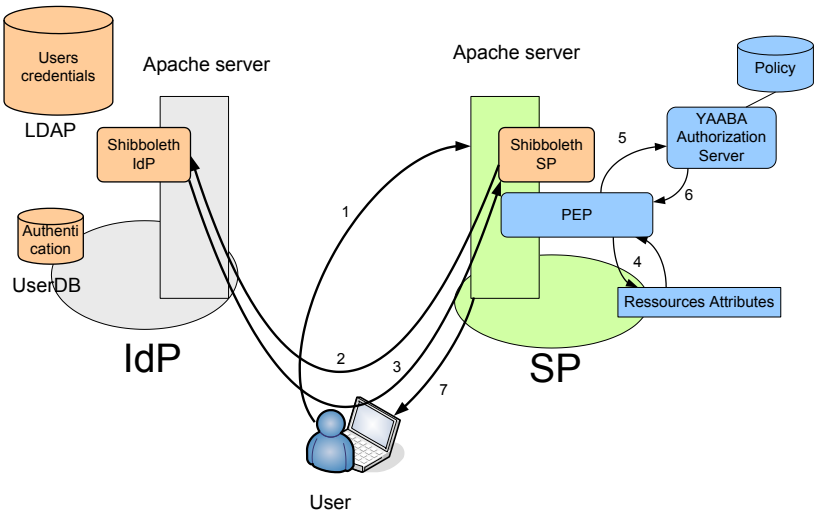


Figure 11. Intégration d'une fédération d'identité et d'un système d'autorisation XACML

Nous avons aussi traité le problème d'un point de vue organisationnel dans (Nasser et al. 2005; Kamel et al. 2008; Kamel et al. 2009). Lors de la construction d'une organisation virtuelle, il faut déterminer quelle entreprise joue le rôle de fournisseur d'identité et/ou fournisseur de service (ce qui inclut la gestion des accès à ce service).

Supposons maintenant qu'une PME n'ait pas les moyens/la capacité de mettre en oeuvre efficacement ces activités de sécurité. Par exemples, elle n'a pas les technologies qui lui permettent de le faire, ou alors les administrateurs n'ont pas l'expérience souhaitée ou encore le processus d'accréditation n'est pas adapté aux règles d'accès complexes. De cette situation peuvent naître des affectations ou des accréditations erronées au niveau de la PME. Une entité peut recevoir des accréditations qui n'ont pas lieu d'être, un système d'authentification invalide laisse échapper une usurpation d'identité, etc. Au final, cela va dégrader le niveau de sécurité global de toute l'organisation virtuelle. Dans ce cas, il est plus judicieux que la PME ne gère pas les identités de ses employés ou l'accès à une ressource partagée.

Pour traiter ce problème, nous avons adopté le concept de meilleures pratiques définies par les normes ISO 27001 et ISO 27002 auquel nous avons intégré le concept de niveau de maturité en se basant sur CMMi. En adaptant ISO 27001 et ISO 27002 au contexte des OVs, nous avons développé un outil pour l'évaluation des pratiques sécuritaires permettant de situer le niveau de confiance porté à un partenaire. Par exemple, les Figure 12 et Figure 13 présentent des extraits des questions portant sur les pratiques liées à la définition d'une politique et à l'authentification. L'outil calcule ainsi le niveau de maturité du partenaire (Figure 14). Ce résultat permet alors de déterminer le ou les rôles que peut jouer le partenaire dans la chaîne de gestion de la sécurité (i.e., gestion des identités et gestion des accès) de l'organisation virtuelle.

Chapter	Section	Subsection	Title	maturity level	Statement
5	**0**	**0**	**Security Policy**		
5	1	0	*Information security policy*		
5	1	1	Information security policy		
5	1	1	Information security policy document	1	A limited number of policies specific to some topics are defined and they are communicated to users in an informal way, no global policy is defined
5	1	1	Information security policy document	2	Some of the organization information security policies are written
5	1	1	Information security policy document	2	Individual managers develop individual policies covering parts of the information security
5	1	1	Information security policy document	3	Security policy document is written and management approval is obtained for the documented policies
5	1	1	Information security policy document	3	The organization has defined a program for the communication of its security policy to its employees
5	1	1	Information security policy document	4	Security level measurement exists
5	1	1	Information security policy document	4	The Security policies controlling information exchange between the organization and its partners are documented and communicated to its employees and partners
5	1	1	Information security policy document	5	Non-compliances with the organization information security policy are automatically reported to take action
5	1	1	Information security policy document	5	The organization stakeholders receive a formal training about the organization security policy, they also know their responsibilities to ensure the organization security

Figure 12. Les questions du contrôle « document de la politique de sécurité de l'information »

Chapter	Section	Subsection	Title	maturity level	Statement	Eval(1;0;0,5)
11	**0**	**0**	**Access Control**			
11	4	0	*Network access control objective*			
11	4	2	User authentication for external connections			
11	4	2	User authentication for external connections	1	Remote users authenticate themselves when accessing the organization network through dial-up methods	
11	4	2	User authentication for external connections	2	Remote users must authenticate themselves through strong authentication mechanisms such as hardware tokens or biometric techniques when accessing the organization network and services	
11	4	2	User authentication for external connections	2	The user authentication mechanisms and methods are selected based on the results of a detailed risk assessment of the level of the required protection	
11	4	2	User authentication for external connections	3	User authentication is logged and logs are reviewed weekly	
11	4	2	User authentication for external connections	3	Compliance of practices with the organization user authentication policy is checked on a regular basis	
11	4	2	User authentication for external connections	4	A Public Key Infrastructure (PKI) is deployed on the organization site	
11	4	2	User authentication for external connections	4	A Single Sign On (SSO) system is deployed on the organization site	
11	4	2	User authentication for external connections	5	Control mechanisms are reviewed and tested continually	

Figure 13. Les questions du contrôle « authentification des utilisateurs pour connexions externes »

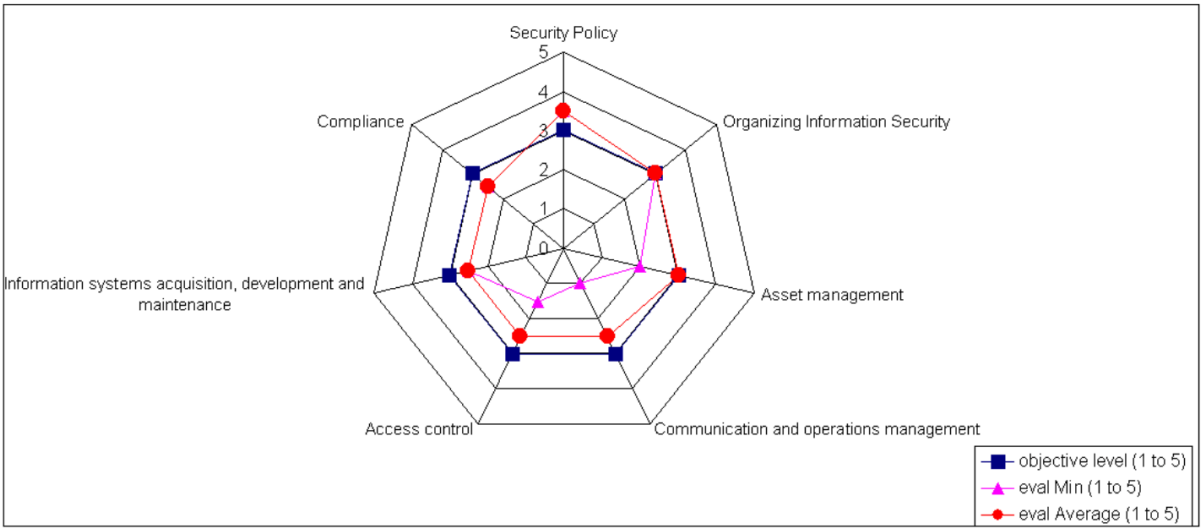


Figure 14. Niveau de maturité des pratiques sécuritaires d'une organisation

2.6 Vers une gestion de la sécurité dynamique et unifiée

Lors du projet PREDYKOT, nous avons amélioré les travaux précédents en approfondissant deux points : la dynamicité et la gestion des configurations.

Les outils de supervision (tels que les sonde SNMPs, les fichiers de logs, les sondes IDS, etc.) fournissent des informations sur l'état actuel de l'infrastructure gérée. Or aujourd'hui les mécanismes de mise œuvre de la sécurité sont très peu couplés aux mécanismes de supervision alors qu'une même exigence de sécurité peut être mise en œuvre différemment selon l'état de l'infrastructure. Lors du projet VIVACE, nous avions déjà mis en œuvre des permissions dynamiques selon l'état d'un workflow en ajoutant un attribut. Cependant, cette solution étant spécifique à notre cas d'utilisation, nous avons donc généralisé cette approche en gardant pour objectif de rendre les permissions/configurations de sécurité dynamiques sans avoir à modifier la politique.

Afin de mieux appréhender ce problème, nous nous sommes tournés vers les travaux liés à l'informatique contextuelle (context-aware computing) et en particulier la définition de Dey (Dey 2001): « Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves. » Ainsi dans notre problématique où l'entité est le système géré, le contexte correspond à toutes les informations de gestion incluant les évènements de supervision dont on dispose. Le concept de *situation* est aussi intéressant à considérer car il donne du sens aux évènements produits par l'activité de supervision. Il permet de raisonner en terme d'états du système en faisant abstraction des évènements bas niveau. Il simplifie donc la spécification de politiques de sécurité considérant la dynamique de l'environnement géré. Nous avons donc introduit la notion de situation dans les politiques de sécurité.

En reprenant la définition de Dey, la situation du système géré est alors calculée par rapport aux contexte de gestion et donc par rapport aux informations de supervision recueillies. Nous avons implanté un gestionnaire de situation dont le rôle est d'identifier ces situations. Pour cela, nous nous sommes basés sur les techniques de traitement des événements complexes (Cugola et al. 2012) qui permettent de manipuler les évènements afin de calculer des évènements de sécurité complexes mais aussi de calculer les débuts et fins de situations. Enfin, nous avons étudié la structuration des politiques orientées par les situations dans le formalisme du contrôle d'accès à base d'attributs et plus particulièrement XACML (Kabbani, Laborde, Barrere, et al. 2014). La Figure 15 montre notre boucle de gestion.

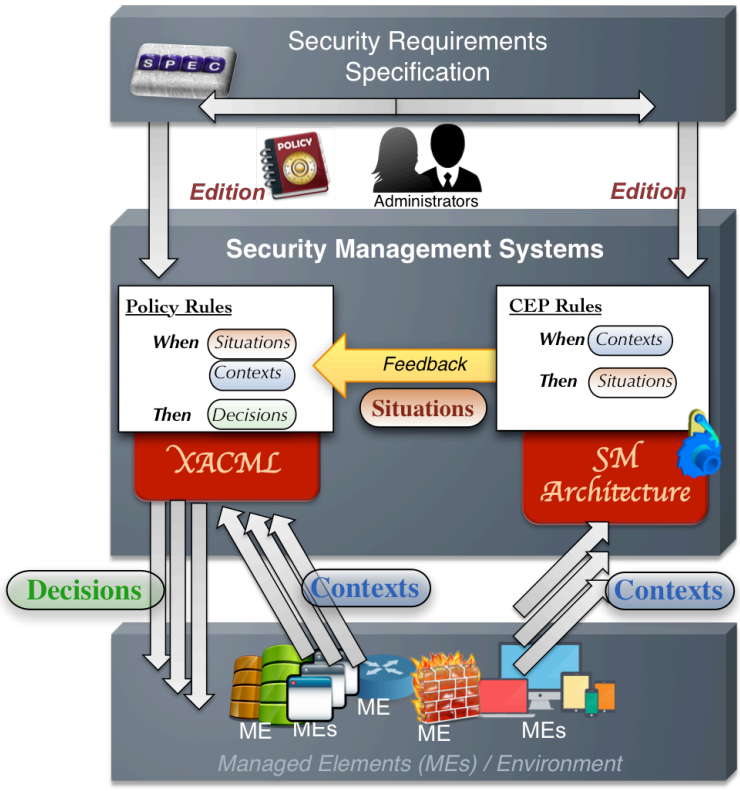
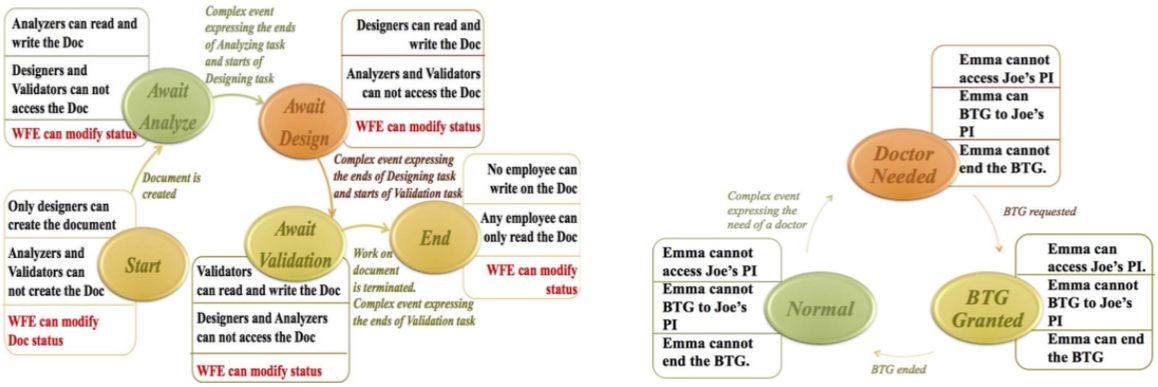


Figure 15. Expression de politiques avec des situations

Nous avons pu montrer la généricité de notre approche orientée situation au travers de différents exemples nécessitant des permissions et des obligations dynamiques. Par exemple, nous avons pu traiter un scénario de type « break the glass » (Kabbani, Laborde, Barrère, et al. 2014), qui consiste à permettre aux médecins de « casser les permissions d'accès aux dossiers des patients » dans les environnements d'e-santé en cas d'urgence médicale, en suivant la même méthodologie que pour notre scénario de permissions dynamiques cadencés par un workflow dans une organisation virtuelle. Dans la Figure 16, les ronds correspondent aux situations, les flèches aux évènements de transition entre situations, et les rectangles correspondent aux droits actifs dans chaque situation. Ainsi, à la Figure 16(a) chaque situation représente les étapes du workflow et les transitions entre situations sont simplement des évènements générés par le *conductor* (noté ici WFE pour workflow engine). Dans le

cas du scénario break the glass (Figure 16(b)), les situations correspondent à l'état du patient. Dans ce scénario, les débuts et fins de situation sont calculés par rapport à différents capteurs indiquant l'état de santé du patient ou des évènements générés par des médecins.



(a) Scénario du workflow

(b) Scénario de break the glass

Figure 16. Analyse de politique de sécurité avec des situations

Exprimer des politiques de gestion en terme de situations permet de prendre en compte la dynamique de l'environnement géré sans avoir à modifier la politique. Nous tenons à ce que la politique ne change pas pour deux raisons. Tout d'abord, pouvoir modifier la politique correspond à avoir des droits d'administrateurs. Or si l'on donne des droits d'administrateur à des utilisateurs qui ne sont pas des administrateurs alors on ne respecte plus un des principes de base de la sécurité qui est le principe des moindres privilèges (Saltzer et al. 1975), i.e. un utilisateur n'a que les permissions qui correspondent aux besoins métier liés à sa fonction et pas plus. La deuxième raison est qu'une politique qui est modifiée dynamiquement dans le temps va devenir incontrôlable. Comment analyser les règles courantes ? Par exemple, l'ordre des règles dans une politique peut être important selon l'algorithme de résolution de conflit qui a été choisi (la première règle, la dernière, la dernière ajoutée, etc.). Donc si l'on veut ajouter des règles dans une politique existante, il faut tenir compte de l'algorithme choisi et des règles déjà existantes dans la politique. Enfin, l'approche orientée situation impose de considérer les états du système géré au moment de la définition de la politique de sécurité et donc de formaliser la dynamique du système tôt dans le processus de sécurisation.

Nous avons complété ce travail par une architecture orientée événements qui couvre de manière unifiée les approches de gestion des autorisations comme des configurations (obligations) selon le modèle de contrôle en externalisation comme en approvisionnement (Figure 17). Considérer les messages de gestion en terme d'évènements, nous permet d'être indépendant de tout protocole de gestion mais aussi de pouvoir intégrer facilement un nouvel agent de gestion. Ces derniers résultats nous permettent de gérer via des politiques conformes au standard XACMLv3 à la fois des autorisations dynamiques où les politiques sont stockées au niveau du PDP mais aussi des configurations à déployer dynamiquement sur des équipements.

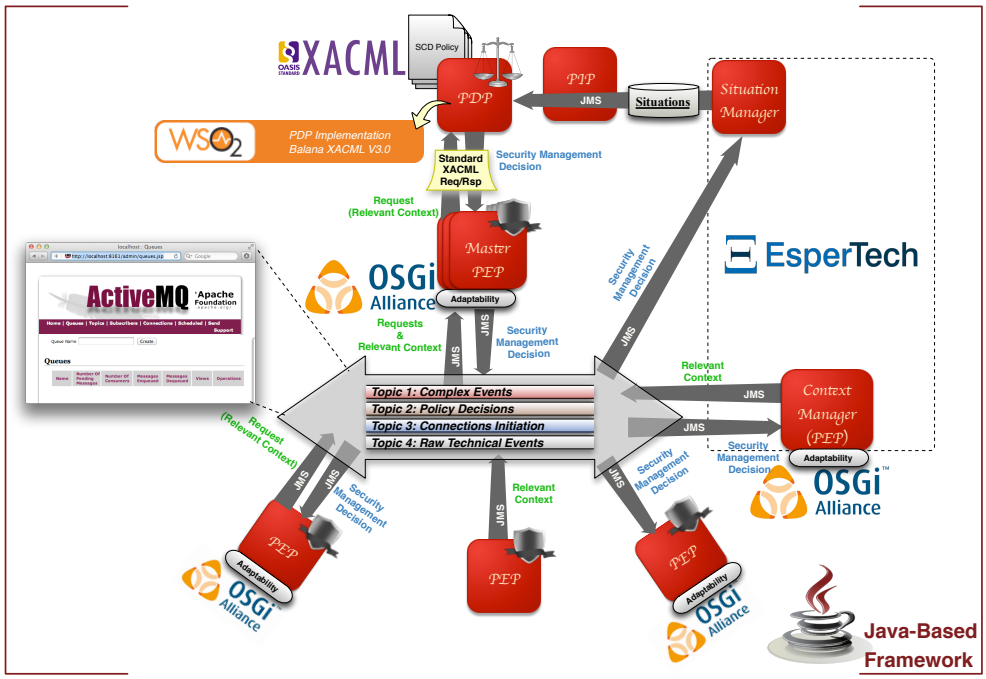


Figure 17. Architecture unifiée pour la gestion de la sécurité

2.7 Bilan

J'ai présenté dans ce chapitre une partie de nos activités sur la gestion des identités et des accès. Elles traitent de l'expression de politiques en utilisant l'approche ABAC et de la mise en œuvre au travers du paradigme de la gestion à base de politique (Figure 18). Nous nous sommes aussi attachés à dynamiser la gestion en connectant l'activité de supervision avec les tâches de réalisation d'une politique de sécurité. Enfin, nous avons développé différents cadres méthodologiques afin de réaliser une telle boucle de gestion dans le cadre des infrastructures virtuelles. Ces travaux ont tous été validés au travers d'implémentations prouvant leur faisabilité. De plus, nous avons participé à différents projets nationaux (GeoWine) et européens (ENHANCE, CASH, VIVACE, PREDYKOT) où nous avons pu confronter nos travaux avec des cas pratiques provenant de partenaires industriels.

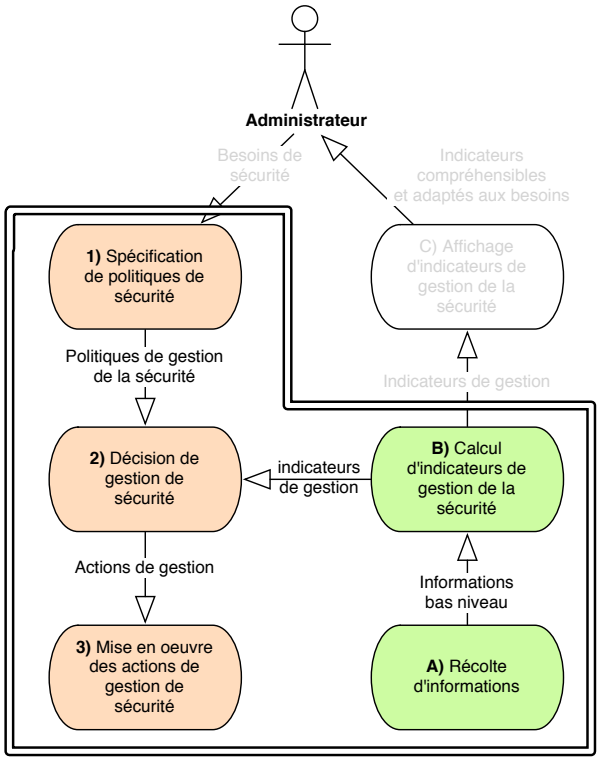


Figure 18. Eléments de la boucle de gestion traités dans le chapitre 2

Outre la valorisation par le biais de publications, j'ai aussi participé à la rédaction d'un document de standardisation d'un protocole de communication entre PDP et PEP dans les grilles publié par l'Open Grid Forum sous le code GFD-P-REC-159 (Chadwick et al. 2009).

J'ai pu acquérir une expérience importante dans la gestion de la sécurité à la fois sur le plan conceptuel avec l'analyse de besoins de sécurité mais aussi sur le plan pratique avec de nombreux prototypes. Cette expérience m'a permis de raffiner notre approche de gestion de la sécurité dont les fondements sont l'expression de politique à base d'attributs et le paradigme de gestion à base de politique. Elle m'a aussi permis de vérifier que ces fondements sont solides car nous n'avons pas eu à changer de paradigme ni pour l'expression, ni la mise en œuvre.

Nous continuons à viser une gestion des identités et des accès dynamiques afin de répondre aux besoins actuels des usagers. Nos futurs travaux doivent permettre de mieux maîtriser le concept de situation. Par exemple, est-il possible de structurer hiérarchiquement des situations comme on le fait pour les rôles et ainsi faciliter l'écriture de politiques orientée par les situations ? Le calcul des situations doit aussi être prédictif, et non réactif comme nous le faisons aujourd'hui, afin d'anticiper le passage d'une situation à une autre. La notion de confiance dans une situation est aussi importante à examiner. L'autre aspect important traite de l'utilisation des obligations. Nous avons démontré que nous pouvions exprimer à la fois des exigences de sécurité (par exemple, la gestion d'un nuage informatique pour l'E-gouvernement) mais aussi gérer des configurations dans la thèse de B. Kabbani (Kabbani 2015). Dans le même esprit, des travaux ont été proposés par d'autres chercheurs pour améliorer la prise en compte des obligations dans XACML comme (El Kateb et al. 2014)

Enfin, si mon expérience sur le plan conceptuel a eu un impact sur le plan pratique, l'inverse est aussi vrai. En effet, je me suis rendu compte en implémentant des systèmes de gestion qu'il y avait un écart important entre la réalité et les propriétés de généricité et la capacité d'extension des systèmes de gestion à base de politique qui sont énoncés à un niveau conceptuel. Ceci m'a poussé à travailler sur l'adaptabilité des systèmes de gestion à base de politique. Cette activité est présentée dans le chapitre suivant.

Chapitre 3. Adaptabilité des systèmes de gestion à base de politique

Ces travaux ont été traités dans le cadre des thèses de Marwan Cheaito (Cheaito 2012), et Bashar Kabbani (Kabbani 2015).

3.1 Présentation de la problèmatique

Le travail présenté dans ce chapitre traite de la définition d'une méthodologie de conception et de développement d'un système de gestion de la sécurité adaptable aux différentes facettes que peut recouvrir la gestion des autorisations et des obligations dans les organisations telles que l'hétérogénéité des pratiques organisationnelles, des technologies utilisées et des contextes à considérer.

Comme je l'ai exprimé précédemment, notre vision se base sur deux approches de gestion : le contrôle d'accès basé sur des attributs et la gestion basée sur des politiques. Le contrôle d'accès basé sur des attributs permet de spécifier des permissions par rapport à toute élément significatif lié aux besoins de sécurité (caractéristiques des utilisateurs, des actions, des ressources et de l'environnement). Cette approche répond aux problèmes liés à l'expressivité des langages de politiques d'autorisation. La gestion à base de politique, quant à elle, vise à permettre l'adaptabilité dynamique du comportement d'un système par le biais de politique de gestion (Sloman et al. 2002; Agrawal et al. 2005). Communément, cette architecture comporte deux entités : le Policy Decision Point (PDP) et le Policy Enforcement Point (PEP). Le PDP est une entité indépendante de l'élément géré, qui prend des décisions de gestion par rapport à une politique donnée. Le PEP fait l'interface entre le PDP et l'élément géré. Lorsqu'une requête est effectuée par un utilisateur sur une ressource, le PEP envoie une demande de décision au PDP et l'applique. Ce type d'architecture favorise l'intégration du système de gestion dans un environnement à gérer. Nous avons donc choisi le standard XACML comme technologie cible car il met en œuvre ces deux approches.

Si d'un point de vue théorique XACML semble répondre aux problèmes d'adaptabilité, les implémentations basées sur ce standard sont limitées à une situation donnée dans la pratique. En effet, un système XACML développé pour des besoins et un environnement technologique donnés ne peut pas être facilement réutilisé dans un autre contexte. Ce problème se retrouve à la fois au niveau du

PDP mais aussi du PEP. Au niveau du PDP, la flexibilité du langage XACML ne permet pas de garantir qu'un PDP donné puisse évaluer une politique écrite en XACML. De même, pratiquement un PEP n'est pas capable de mettre en œuvre toute décision décrite en XACML. Il est donc nécessaire de définir une méthodologie de conception et de développement pour rendre un tel système d'autorisation adaptable dans la pratique.

Notre approche consiste à définir un système d'autorisation minimal qui puisse être facilement étendu pour des besoins spécifiques à une situation donnée (e.g., capacité d'expression et de mise en œuvre de politiques incluant des contraintes complexes, adaptation à environnement technologique particulier, etc). Ceci amène les questions suivantes :

1) Quelles extensions doivent être apportées au système d'autorisation minimal ? Est-il possible de réutiliser des extensions pour différentes situations données ? Par exemple, le nombre de technologies utilisées pour stocker les accréditations des utilisateurs est limité (e.g., LDAP, MySQL, Active Directory). Cependant, les accréditations ainsi que la structuration de ces données d'accréditation peuvent différer d'une organisation à une autre.

2) Comment gérer le cycle de vie des extensions dans le système d'autorisation ? En effet, il existe un lien fort entre l'utilisation d'une extension et les besoins exprimés dans une politique de sécurité. Par exemple, l'existence dans le système d'autorisation d'une extension permettant de récupérer le rôle de l'utilisateur dans une base de données MySQL n'est nécessaire que si le système d'autorisation doit évaluer au moins une politique incluant des contraintes sur le rôle des utilisateurs. Dans le cas contraire, cette extension n'a pas lieu d'être ajoutée au système d'autorisation minimal. De la même manière, si une politique incluant des contraintes sur les rôles des utilisateurs est chargée dans le système d'autorisation, l'extension associée doit être ajoutée.

3.2 Notion d'adaptabilité et mise en œuvre

Je présente dans cette section la notion d'adaptabilité d'un système ainsi que l'approche composants orientés service que nous avons utilisée pour réaliser des entités de gestion adaptables.

3.2.1 Définition d'adaptabilité

Nous nous sommes intéressés aux différents travaux liés au concept d'adaptabilité des systèmes informatiques dans le domaine du génie logiciel. De manière générale, l'adaptation représente le changement d'un système afin de répondre aux variations de son environnement. Devant la multitude de définitions liées à ce concept (Cheaito 2012), nous avons choisi de retenir celle donnée par (Chung et al. 2004) qui est à la fois générique et qui réduit les ambiguïtés par son approche formelle. Selon (Chung et al. 2004), l'adaptation d'un système S est causée par un changement Δ_E intervenu dans un

environnement *E* (consistant à l'environnement d'exécution et les besoins métiers) qui devient un nouvel environnement *E'*. Cette adaptation résulte en un nouveau système *S'* qui idéalement répond aux besoins du nouvel environnement *E'* (Figure 19). Ainsi, l'adaptation peut être représentée par une fonction *Adaptation*: E×E'×S→S', où meet (S', need (E')).

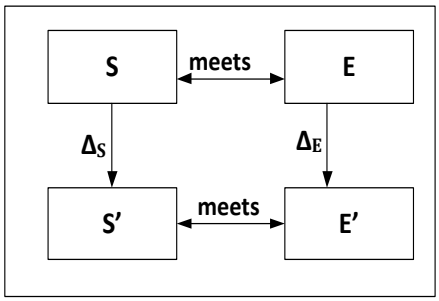


Figure 19. Définition de l'adaptation selon (Chung et al. 2004)

Par conséquent, un système est adaptable si une telle fonction d'adaptation existe, et l'adaptabilité fait référence à la capacité du système à mettre en œuvre cette fonction d'adaptation. La réalisation de cette fonction d'adaptation implique trois fonctionnalités: 1) la capacité de reconnaître le changement d'environnement Δ_E, 2) la capacité à déterminer le changement à apporter sur le système Δ_S, 3) la capacité à effectuer ce changement pour générer le nouveau système *S'*. Ces trois fonctionnalités sont résumées par les fonctions suivantes :

- EnvChangeRecognition : E' × E → Δ_E .

  La fonction *EnvChangeRecognition* représente la capacité d'observation. Cette capacité d'observation doit permettre de détecter les variations de l'environnement. En effet, se sont les variations de l'environnement qui déclenchent les adaptations.

- SysChangeRecognition : Δ_E × S → Δ_S.

  La fonction *SysChangeRecognition* représente la capacité de décision. Cette fonctionnalité doit inclure des mécanismes permettant de définir une adaptation par rapport à une variation de l'environnement.

- SysChange : Δ_S × S → S', où meet(S', need(E')).

  La fonction *SysChange* représente la capacité d'action. Une fois qu'une adaptation a été décidée, il est nécessaire de déterminer les modifications concrètes à réaliser sur le système.

Partant de cette définition, nous avons proposé des solutions pour mettre en œuvre ces trois fonctions et rendre ainsi notre système de gestion adaptable. L'analyse complète d'un système de gestion à base de politique par rapport à la définition de (Chung et al. 2004) a été écrite dans la thèse de Marwan Cheaito (Cheaito 2012). Je ne présenterai ici les besoins d'adaptation qu'à travers d'exemples.

3.2.2 Introduction à l'approche composants orientés services

Pour répondre aux besoins de l'adaptabilité dynamique, nous avons utilisé l'approche de programmation composants orientés services. Elle offre à la fois les avantages d'adaptabilité dynamique, comme l'intégration et de dynamisme des architectures, mais aussi la réutilisabilité et la gestion des dépendances des modèles orientés composants (Cervantes et al. 2004).

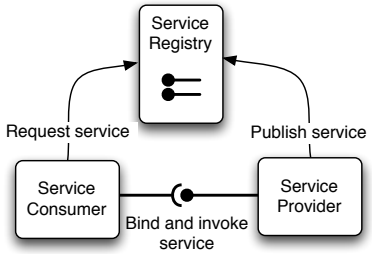


Figure 20. Architecture orientée service

L'architecture orientée services est basée sur l'idée que les applications peuvent découvrir et invoquer des services pour accomplir certaines tâches (Papazoglou et al. 2007). Rappelons que l'approche orientée services est organisée en trois parties (Figure 20) : un fournisseur de service, un consommateur de service et un annuaire de services. Un annuaire de services typique se compose d'un ensemble d'entités donnant la possibilité d'accéder et de récupérer les informations sur les services d'intérêt (Tsai et al. 2007) pour des parties externes ou des consommateurs de services. Les fournisseurs de services publient leurs services à tout moment dans l'annuaire et les consommateurs de services peuvent invoquer un service fournisseur enregistré dans le service annuaire pour un contrat ou propriété spécifique. En plus, l'approche orientée services permet aux services consommateurs d'être notifiés de façon dynamique des nouveaux services fournisseurs enregistrés dans le service annuaire. Cependant, la programmation composants orientés services traite de la réutilisabilité de blocs logiques de programmes qui implémentent une ou plusieurs interfaces. Un logiciel orienté composants est un assemblage de composants. La notion d'interface étant très similaire à la notion d'interfaces de service, la programmation orientée composants a été utilisée pour mettre en œuvre des services ; un service pouvant être mis en œuvre par un ou plusieurs composants.

3.3 Adaptabilité du moteur de décision

XACML est un langage dans lequel les règles d'autorisation sont des expressions sur des attributs. Chaque attribut est identifié par un URN (Uniform Resource Name) et possède un type de données lui même représenté par un URN. Les attributs sont manipulés via des fonctions qui ont leur propre URN. La spécification XACML proposée par OASIS définit des attributs (par exemple, le nom du sujet) ainsi que des types de données et des fonctions associées (par exemple, le type 'chaîne de caractères' et la fonction 'égalité'). Une implémentation conforme à XACML doit donc mettre en œuvre les URNs du standard.

Toutefois, comme son nom l'indique (« eXtensible Access Control Markup Language »), XACML peut être étendu. Ainsi si l'on désire manipuler un attribut non-standard, il suffit de choisir un URN pour pouvoir exprimer une règle définissant des contraintes sur cet attribut. De même, il possible d'étendre les expressions XACML par de nouveaux types de données et de nouvelles fonctions en utilisant de nouveaux URNs.

Cette capacité d'extension facilite la spécification de politiques de sécurité et permet au langage de s'adapter aux besoins métiers. Cependant, elle pose aussi un problème de déploiement car il se peut qu'un PDP standard ne sache pas interpréter les URNs ajoutées et donc ne puisse pas prendre de décision. Par conséquent, des ajouts au langage peuvent nécessiter d'étendre le code du PDP posant un problème de consistance du système de gestion.

3.3.1 Besoins d'adaptation du PDP

Je présente ici un exemple pris de (Laborde et al. 2010) afin de comprendre la problématique liée au déploiement d'un système d'autorisation XACML dans un environnement réel. Cet exemple se focalise uniquement sur le côté moteur de décisions de politiques ou PDP.

Considérons une entreprise, appelée « MY-ORGANIZATION », qui décide d'installer un service web cartographique. Ce service peut fournir des cartes insérées par l'entreprise et en particulier des vues détaillées de ses bâtiments. Cette entreprise désire restreindre l'accès à ces vues détaillées uniquement à ses employés. Tous les comptes utilisateurs sont déjà stockés dans une base de données « MySQL ». Les employés qui travaillent pour cette entreprise peuvent provenir de différentes entreprises et en particulier de sous-traitants. Pour différencier les employés, les comptes utilisateurs possèdent un champ appelé « organization-name » qui contient le nom de l'entreprise d'origine.

Pour construire sa politique, l'administrateur de sécurité désire utiliser le profil « GeoXACML », dont il connait l'existence (développé par l'OGC (Matheus et al. 2008)). En effet, ce standard propose des types de données et des fonctions pour manipuler des données géographiques dans des politiques XACML. La politique de sécurité du scénario proposé est la suivante : « Si l'attribut de l'utilisateur « organization-name » est égal à « my-organization » et que la zone géographique demandée (attribut de la ressource « requested-area ») se trouve dans la zone « MY-ORG-AREA » alors accepter ; sinon refuser l'accès ».

Le processus d'exécution est alors le suivant (Figure 21). L'administrateur écrit sa politique en XACML et la charge dans le PDP via le Policy Administration Point (PAP) (étapes 1 et 2 dans Figure 21). Quand un utilisateur tente d'accéder à une carte, le PEP intercepte la requête de l'utilisateur et génère une requête XACML qu'il envoie au PDP (étape 3 dans la Figure 21). Cette requête contient les valeurs pour les attributs « subject-id » et « requested-area ». Dans notre exemple, l'attribut « organization-name » n'est pas envoyé par le PEP.

Lorsque le PDP évalue la politique, il doit faire appel au module Policy Information Point (le PIP est l'entité XACML chargée de récupérer des valeurs d'attributs non présents dans le contexte de

requête du PEP) pour l'obtenir depuis la base de données MySQL (étape 4 dans Figure 21). Ceci implique que l'implémentation XACML doit intégrer un code PIP implémentant les requêtes MySQL et qu'il possède la configuration nécessaire pour accéder au serveur MySQL (comme l'adresse du serveur, login, le mot de passe, le schéma de la base ou la requête SQL). Ensuite, le PDP évalue la fonction « geometry-contains ». Ceci implique que le PDP doit avoir aussi le code qui implémente cette fonction, et ainsi le code pour le type de données associé à cette fonction (étape 5 dans Figure 21). Finalement, le PDP retourne sa décision au PEP (étape 6 dans Figure 21).

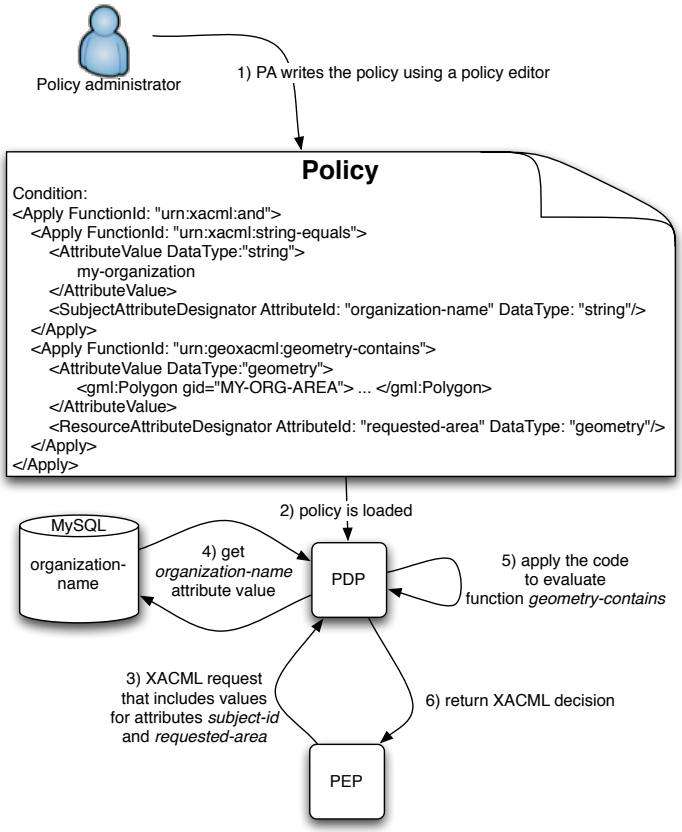


Figure 21. Exemple de politique non interprétable par un PDP standard

Cet exemple montre qu'étendre le langage XACML n'est pas si simple. En effet, les notations, au format XML devraient être accompagnées du code permettant au PDP d'interpréter ces écrits (dans le cas présent un nouveau code pour le type de données GeoXACML et sa fonction et un nouveau code pour le PIP MySQL). Les changements du système sont dans ce cas causés par des variations du langage de politique XACML ; ici, à l'extension du langage de politiques par un nouveau type de données et/ou un nouvel attribut PIP. Par conséquent, cette situation implique d'effectuer des adaptations sur le PDP avec des codes supplémentaires pour prendre en compte le nouveau type de données et/ou le nouvel attribut PIP.

3.3.2 Le concept de politique auto-contenue

Il existe certaines implémentations de XACML où il est possible d'ajouter de nouvelles fonctionnalités à un PDP et cela à la volée, comme HERASAF (« HERAS-AF Homepage » 2015). Cependant, il reste le problème de gestion de ces extensions. Qui ajoutera ces modules ? Qui supprimera les modules lorsqu'ils ne seront plus utilisés ? De plus, lorsqu'un administrateur écrit sa politique XACML, il doit toujours s'assurer que le PDP cible possède les extensions nécessaires à sa politique. Lorsque le système de gestion ne comprend qu'un unique PDP, gérer cette compatibilité manuellement est envisageable. Cependant, cette approche n'est plus concevable dans un environnement comprenant plusieurs PDPs.

Nous avons mis en avant le lien fort qui existe entre une politique et le PDP qui doit l'interpréter. Nous avons donc proposé le concept de « politique auto-contenue » (Cheaito et al. 2010a). L'originalité de notre idée vient du fait que la politique doit contenir tous les éléments nécessaires pour permettre à un PDP de l'évaluer et nous avons formalisé ceci au travers de trois critères :

- Propriété d'auto-suffisance : Une politique auto-contenue doit contenir toutes les informations nécessaires à son évaluation par un PDP. Par exemple, la politique auto-contenue doit inclure le code et la configuration des PIP, la structuration et la configuration de données non standard afin que le moteur de décisions d'autorisation soit capable d'interpréter et d'exécuter la politique avec ses extensions.
- Propriété d'auto-description : Une politique auto-contenue doit fournir assez d'information pour la gestion de son cycle de vie. La politique auto-contenue doit fournir une description des éléments qu'elle contient (i.e. PIP, fonctions, données...) et la façon de les utiliser, la liste des éléments qui doivent être installés pour son exécution. Le chargement d'une politique est réalisé en tenant compte de ces informations. De même lorsqu'une politique est supprimée, la description sera utilisée pour décider des modules qui doivent être enlevés par le moteur d'autorisation.
- Propriété de dynamicité : Une politique auto-contenue doit pouvoir être chargée et retirée dynamiquement. Cette exigence découle de la définition fondatrice de la gestion à base de politiques dans (Sloman et al. 2002). Le système doit être capable de charger et décharger dynamiquement une politique auto-contenue sans avoir besoin d'arrêter ou de recoder le système.

3.3.3 Mise en œuvre de politique auto-contenue

Je présente ici notre architecture de déploiement de politique auto-contenue satisfaisant nos trois propriétés et répondant à l'approche de programmation service orientée composants (Figure 23). Dans cette architecture, nous différencions le PDP du moteur d'autorisation. Le PDP ne considère que le

fichier politique XACML. Le moteur d'autorisation est l'environnement complet d'exécution de politiques auto-contenues.

Une politique auto-contenue comprend trois types de composants : les composants d'accès à la politique (Policy Access), les composants PIP et les composants types de données :

- Policy Access : Le composant d'accès à la politique fournit un seul service, appelé « Get- policy », permettant au PDP d'accéder aux fichiers politiques XACML. Lorsque le composant PAP active la politique auto-contenue dans le moteur, ce service est automatiquement enregistré. Le PDP est alors notifié qu'il peut charger les politiques XACML pour pouvoir l'utiliser afin de mettre en œuvre le processus de décisions d'autorisation.
- PIP : Les composants PIP sont dédiés à la récupération d'attributs dont il faut connaitre la valeur mais qui ne figurent pas dans le contexte de requête XACML. Ils peuvent provenir de plusieurs sources. Les composants PIP publient le service « Get-attribute » qui ajoute les couples <attribut, valeur> dans le contexte de requête. Un composant PIP peut être responsable d'un ou plusieurs attributs. En conséquence, chaque PIP doit indiquer le nom du ou des attributs (en XACML il s'agit d'un URN) dont il est à charge. De plus, le fichier de configuration du PIP contient toutes les informations nécessaires pour que le composant PIP soit capable d'extraire et de transformer toutes les valeurs de l'attribut au format attendu ou requis par le type de donnée de cet attribut.
- Data Type : Les composants de type de données implémentent les types de données et les fonctions non standard utilisées dans la politique XACML. Les composants type de données doivent fournir les services pour permettre au composant PDP d'évaluer les expressions dans la politique grâce au service « Evaluate-expression ». Ils indiquent au PDP l'ensemble des fonctions (le nom d'une fonction est un URN unique dans XACML) qu'ils implémentent dans le contrat de service. Il n'est pas nécessaire d'indiquer les types de données pris en charge car XACML est un langage préfixé. Ainsi, dès que le PDP trouve une fonction non standard dans la politique, il invoque le service associé à cette fonction en lui passant en paramètre tout le bloc d'expression à évaluer. Ce processus est récursif. Si le composant pour la fonction « XYZ » trouve une sous expression <Apply FunctionId:"urn:ABC">...</Apply>, il peut invoquer le service associé à cette fonction de la même manière, etc. Tout comme les composants PIP, les composants type de données peuvent nécessitent des informations qui résident dans des fichiers de configurations du type de données qu'il implémente (Cheaito et al. 2010b)).

Le moteur d'autorisation manipule les politiques auto-contenues et comprend trois entités actives : le PDP, le Context-Handler et le PAP. D'autre part, le composant « Core Authz Decision Access Point » est un point d'accès entre le PEP et le moteur d'autorisation :

- L'entité PDP qui est un moteur de décision d'autorisation. Le rôle du composant PDP est similaire à celui présent dans l'architecture XACML c.à.d. la prise de la décision d'autorisation en évaluant les politiques avec des requêtes. Il fournit le service « Get-decision » pour donner les décisions d'autorisation prises.
- Le Context-Handler récupère la requête XACML d'une entité du composant « Core Authz Decision Access Point ». Ensuite, il fournit le service « Get-XACML-request » pour donner la requête XACML aux autres composants.
- Le rôle du PAP est de gérer le cycle de vie de la politique auto-contenue en fournissant le service « PAP-admin » qui est responsable de :
  1) Charger une politique auto-contenue : le PAP charge tous les composants de la politique dans le moteur d'autorisation. Cependant, les services ne sont pas enregistrés dans l'annuaire à cette étape ;
  2) Activer une politique auto-contenue : le PAP active tous les composants de la politique qui s'enregistrent dans l'annuaire et le PDP est notifié qu'il peut exécuter la politique ;
  3) Désactiver une politique auto-contenue : Les services sont supprimés de l'annuaire et le PDP n'exécute plus la politique ;
  4) Supprimer la politique auto-contenue : les composants de la politique auto contenue sont enlevés de l'environnement du moteur d'autorisation.

Nous avons implémenté cette architecture dans le cadriciel OSGi et des évaluations de performances ont démontré que notre approche était viable (Cheaito et al. 2010a). Pour cela, nous avons étudié les deux prototypes suivants pour tester l'impact en terme de performance de l'utilisation OSGi:

- Le premier prototype est basé sur l'implémentation SUNXACML (Sun XACML 2016), qui fournit une API Java pour ajouter de nouvelles fonctions, types de données et les PIPs. Nous appelons ce prototype « *Classic XACML* »
- Le second prototype est notre implémentation OSGi de composants orientée services pour des politiques auto-contenues. Nous appelons ce prototype « *OSGi XACML* ».

Afin de valider notre approche, le PDP est basé sur SUN XACML dans les deux cas. Le code qui implémente les fonctions de types de données non-standard et le PIP est le même. Pour chaque test, nous avons mesuré le temps moyen pour prendre une décision de contrôle d'autorisation en millisecondes basé sur 1000 requêtes.

Notre expérimentation a consisté en trois tests (voir Figure 22):

- **Test1 - type de données non standard:** La politique contient un type de données non-standard et la fonction. Dans ce test, aucun PIP n'est nécessaire.
- **Test2 - appel d'un PIP:** Dans ce cas, un attribut est manquant dans la requête XACML. Le PDP appelle un PIP pour obtenir les valeurs d'attribut dans une base de données MySQL. Les types de données et les fonctions utilisées dans la politique sont inclus dans le standard XACML.
- **Test3 - type de données non standard et appel d'un PIP:** Dans ce cas, nous avons testé la réaction du PDP avec une politique qui contient une expression avec une fonction non-standard. En outre, l'expression contient une contrainte sur une valeur d'attribut qui n'est pas dans le contexte de la requête XACML. Ainsi, le PIP est appelé pour obtenir cette valeur à partir d'une base de données MySQL.

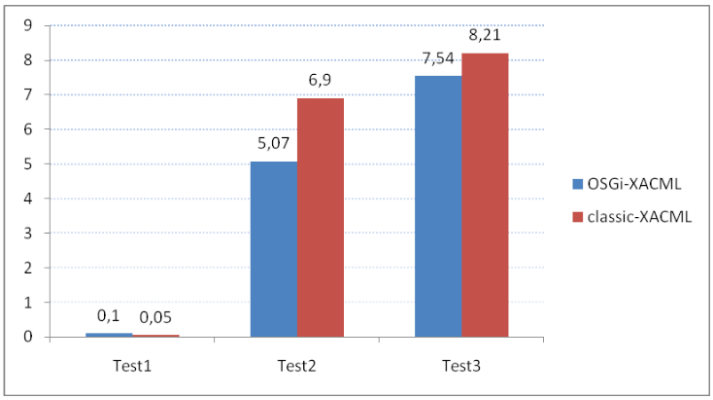


Figure 22. Performance politique auto-contenue - Temps pour chaque test en millisecondes

Notre travail sur cette architecture de moteur d'autorisation avait pour objectif la réutilisation du code. Nous avons donc aussi étudié la réutisation des modules PIP et Data Type (Cheaito et al. 2010b) afin que l'activité d'édition de politiques auto-contenues puisse correspondre à 1) choisir un module parmi une liste de modules disponibles, 2) configurer le module, et 3) ajouter le module dans la politique auto-contenue et utiliser les fonctionnalités implémentées par le module dans la politique XACML. Nous avons développé un environnement intégré d'édition de politiques auto-contenues construit sur Netbeans pour faciliter cette tâche (plus de détails sont disponibles dans (Cheaito 2012)). Notre architecture permet d'envisager d'autres utilisations d'un système d'autorisation. Nous avons par exemple étudié la possibilité de fournir l'autorisation comme un service par un fournisseur (Authorization-as-a-Service) (Laborde et al. 2013).

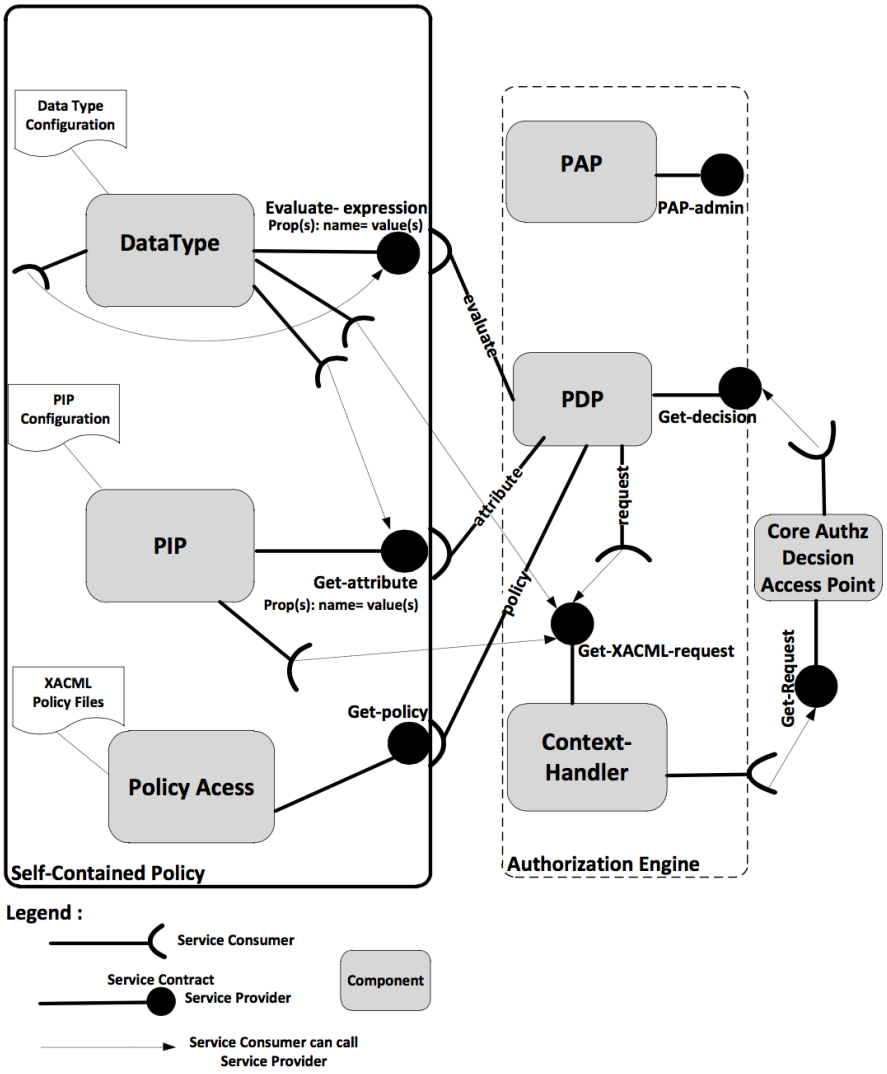


Figure 23. Architecture de déploiement de politiques auto-contenues

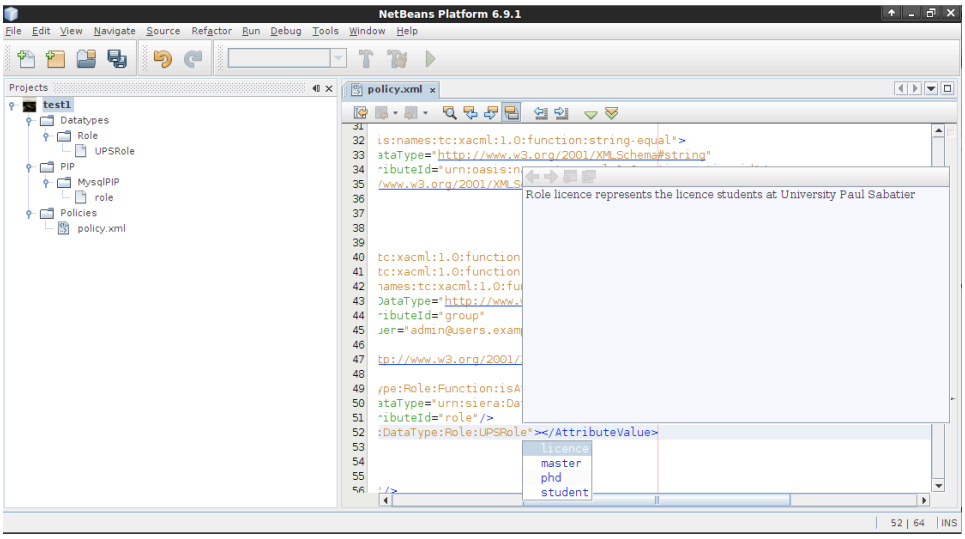


Figure 24. Editeur de politiques auto-contenues

Pour reprendre la définition de (Chung et al. 2004), une politique auto-contenue contient Δ_S où S est un PDP standard. L'administrateur détecte qu'il/elle utilise des extensions au moment de l'édition (fonction *EnvChangeRecognition* : $E' \times E \rightarrow \Delta_E$). Lorsqu'il/elle choisit les composants à ajouter dans la politique auto-contenue, il/elle décide de la stratégie d'adaptation (fonction *SysChangeRecognition* : $\Delta_E \times S \rightarrow \Delta_S$). Ainsi le système d'autorisation par le biais du PAP n'a plus qu'à réaliser la fonction *SysChange* : $\Delta_S \times S \rightarrow S'$, où meet(S', need(E')). De plus, lorsque la politique auto-contenue est retirée, le PAP connaît aussi le Δ_S à appliquer grâce à la propriété d'auto-description.

3.4 Adaptabilité de l'agent de mise en œuvre de la politique

La problématique d'adaptabilité se situe aussi au niveau du PEP. En effet, la gestion des permissions a évolué de l'approche classique qui purement gestion des autorisations pour atteindre aujourd'hui le contrôle des usages. Cela a été popularisé par le modèle UCON (Park et al. 2004). Cette nouvelle approche combine la gestion des obligations (Elrakaiby et al. 2012) à la gestion des autorisations afin d'offrir plus de contrôle sur le système. Le contrôle des usages a démontré son efficacité dans divers scénarios tels que la gestion de la protection de la vie privée (Mont et al. 2006), la gestion des nuages informatiques (Danwei et al. 2009) ou encore la gestion d'un réseau (Lymberopoulos et al. 2003). Le standard XACML a suivi cette évolution en généralisant les obligations dans la version 3 de son langage. En effet, XACML permet de spécifier des obligations à tous les niveaux de granularité d'une politique XACML (Ensemble de politiques, politique et règle). Une obligation doit être mise en œuvre par un PEP. Ajouté aux obligations, la version 3 de XACML (OASIS XACMLv3 2013) a introduit les conseils qui peuvent aussi être exprimés à tous les niveaux de granularités d'une politique XACML. Contrairement, un PEP n'est pas obligé de mettre en œuvre un conseil.

D'un point de vue déploiement, cette généralisation de l'utilisation des obligations peut imposer aux PEPs une adaptation. En effet, une obligation correspond techniquement à une fonction que le PEP doit exécuter. Ainsi, il est nécessaire de garantir que chaque PEP possède le code associé aux obligations et sache exécuter ce code.

3.4.1 Besoins d'adaptation du PEP

Je présente l'exemple tiré de (Laborde et al. 2014) pour mettre en lumière les besoins d'adaptation du PEP. Soit une politique permettant aux sujets avec le rôle *R* d'accéder au service *S*. Afin de mettre en œuvre cette politique, un PEP est créé. Celui-ci intercepte les tentatives d'accès au service S, transforme ces tentatives en requêtes XACML, et envoie les requêtes XACML au PDP. Ensuite, il attend la réponse du PDP qui peut être *Permit*, *Deny* ou *Not Applicable* (Figure 25a). Le PEP est programmé de telle sorte que la réponse *Permit* laisse le processus d'accès au service continuer. Les réponses *Deny* et *Not Applicable* sont elles mises en œuvre en bloquant le processus.

```
<Response>
  <Decision>Permit</Decision>
</Response>
```

(a) Réponse envoyée par le PDP sans obligation

```
<Response>
  <Decision>Permit</Decision>
  <Obligations>
      <Obligation ObligationId="urn:siera:example:obligation:log-access:file"
                  FulfillOn="Permit">
  </Obligations>
</Response>
```

(b) Réponse envoyée par le PDP avec obligation

Figure 25. Exemples de réponse XACML

Au bout d'un certain temps, l'administrateur sécurité décide de changer sa politique car il/elle désire enregistrer les tentatives d'accès autorisées. Il/elle modifie sa règle en ajoutant une obligation qui indique au PEP qu'il doit enregistrer les accès autorisés. Les réponses reçues par le PEP deviennent alors comme dans la Figure 25b. Cependant, cette obligation n'existait pas au moment où le PEP a été conçu. Par conséquent, il ne sait pas interpréter l'obligation de la requête. Tout comme, il existe un lien entre la politique et le code du PDP, il existe un lien entre la politique et le code du PEP.

Nous avons donc formulé les exigences suivantes correspondant à notre PEP idéal :

- **Exigence 1** : Un PEP doit être capable de mettre en œuvre toute décision XACML.
- **Exigence 2** : Un PEP doit pouvoir s'adapter dynamiquement. Etant donné que la politique peut évoluer dans le temps amenant de nouvelles exigences, un PEP doit s'adapter à la volée afin de ne pas avoir à stopper le service protégé. Comme pour le PDP, cette exigence découle de la définition fondatrice de la gestion à base de politiques dans (Sloman et al. 2002).
- **Exigence 3** : Un PEP doit rester conforme avec le standard XACML. Nous ne voulons pas créer une nouvelle spécification de système d'autorisation. Par conséquent, le protocole Requête/Réponse ne doit pas être modifié.
- **Exigence 4** : Un PEP doit fournir des interfaces pour être facilement intégré à une application/service. Le PEP correspond à la couche d'intégration du système de gestion des accès avec les ressources protégées. La technologie utilisée pour développer le PEP doit être compatible avec d'autres technologies.
- **Exigence 5** : La fonctionnalité d'adaptation ne doit pas compliquer la tâche de développement d'un PEP. Aujourd'hui, les APIs pour développer des PEPs permettent de demander une décision au PDP à travers des méthodes telles que *getDecision(Requête)*. Il faut garder cette simplicité.

3.4.2 Architecture du PEP adaptable

Nous avons utilisé l'approche de programmation composants orientés service comme pour le PDP pour formuler l'architecture de la Figure 26 qui comprend :

- Le corePEP qui est l'élément central de notre architecture. Ce composant :
  - Communique avec le point d'accès au PDP via le service getDecision
  - Fait appliquer les obligations si besoin en appelant le service applyObligation
  - Installe des modules d'obligation à la volée.
- Le PDPAccessPointImpl. Ce composant permet au PEP de contacter un PDP de diverses manières. En particulier, il correspond au composant CoreAuthorizationAccessPoint de l'architecture du moteur d'autorisation de la Figure 23.
- Les composants implémentant les obligations. Chaque composant obligation publie l'URN de l'obligation qu'il implémente afin que le cœur du PEP puisse appeler le bon composant lorsqu'une obligation doit être réalisée.

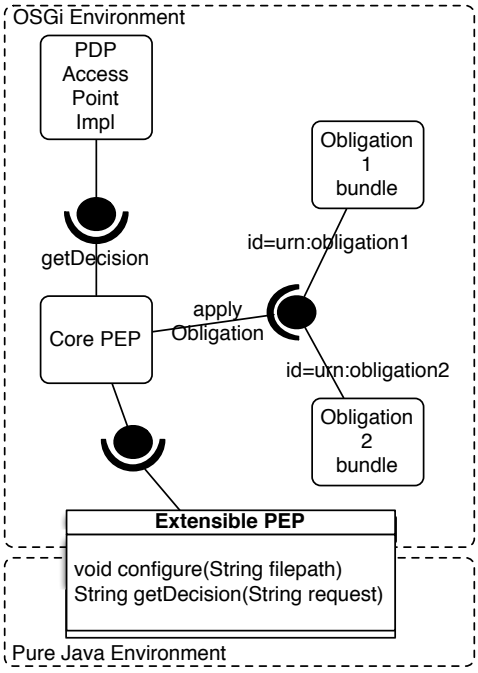


Figure 26. Architecure du PEP adaptable

Nous avons implémenté cette architecture dans le cadriciel OSGi (« OSGi Alliance » 2015). Cependant, faire cohabiter une application OSGi avec une application Java pure n'est pas simple (Hall et al. 2011) (e.g., les chargeurs de classes sont différents). Ceci pose un problème d'intégration d'un PEP OSGi dans une application existante (Exigence 4). Nous avons donc créé une classe ExtensiblePEP qui lance un environnement OSGi personnalisé rendant transparente la communication entre une application Java et le CorePEP.

3.4.3 Expression et réalisation de l'adaptation

Le composant CorePEP peut installer de nouveaux composants obligation. Il faut compléter cette fonctionnalité par un mécanisme qui informe le PEP sur : 1) quel composant implémente quelle obligation, et 2) comment installer et configurer ces composants. Nous avons décidé d'exprimer ces informations dans la politique directement. XACMLv3 intègre le concept de conseil qui complète les obligations. De plus, d'après le standard XACMLv3, les conseils peuvent être ignorés par le PEP. Par conséquent, cela nous a semblé être un bon moyen de communication pour informer le PEP quant à l'installation et l'utilisation de composants obligation. Le deuxième bénéfice apporté par cette approche est que les conseils sont envoyés en même temps que les obligations sans modification du protocole Requête/Réponse utilisé dans XACML.

Nous avons proposé d'utiliser deux types de conseils pour mettre en œuvre des obligations. Le premier type de conseil, que nous appelons *conseil d'installation*, fournit les informations nécessaires pour retrouver le composant obligation. L'URN de ce conseil doit être *urn:siera:management:obligation.* Un conseil d'installation comprend trois attributs : i) l'attribut *urn:siera:obligationId* indique l'URN de l'obligation utilisé dans la politique, ii) l'attribut *urn:siera:bundle:file:location* indique la localisation du composant, et iii) l'attribut *urn:siera:bundle:file:name* contient le nom du fichier du composant. Par exemple, le conseil de la Figure 27 (ligne 97) décrit que l'obligation *urn:siera:example:obligation:log-access:file* est implémentée par le composant *FileAccessLog_1.0.0.201306191231.jar* qui se ici trouve dans le répertoire local *obligation-store.* Il est tout à fait possible que le composant soit stocké sur une machine distante. Ainsi, lorsque le PEP reçoit la réponse du PDP incluant une obligation, il sait où télécharger le composant correspondant. Le deuxième type de conseil est appelé *conseil de configuration*. Ces conseils donnent la configuration du composant obligation. Contrairement aux conseils d'installation qui sont utilisés par le PEP, les conseils de configuration sont pris en compte par le composant obligation. La seule contrainte sur les conseils de configuration est que l'URN doit être la même que celui de l'obligation. Les attributs du conseil de configuration dépendent quant à eux du composant obligation. Dans l'exemple de la Figure 27 (ligne 115), le composant de l'obligation *urn:siera:example:obligation:log-access:file* doit effectuer ses enregistrements dans le fichier */var/log/siera/file.log*.

```
<ObligationExpressions>
    <ObligationExpression ObligationId="urn:siera:example:obligation:log-access:file" FulfillOn="Permit">
</ObligationExpression>
</ObligationExpressions>
<AdviceExpressions>
    <!-- Advice for installing the component -->
    <AdviceExpression AdviceId="urn:siera:management:obligation" AppliesTo="Permit">
        <AttributeAssignmentExpression AttributeId="urn:siera:obligationId">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                urn:siera:example:obligation:log-access:file
            </AttributeValue>
        </AttributeAssignmentExpression>
        <AttributeAssignmentExpression AttributeId="urn:siera:bundle:file:location">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                obligation-store/
            </AttributeValue>
        </AttributeAssignmentExpression>
        <AttributeAssignmentExpression AttributeId="urn:siera:bundle:file:name">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                FileAccessLog_1.0.0.201306191231.jar
            </AttributeValue>
        </AttributeAssignmentExpression>
    </AdviceExpression>
    <!-- Advice for configuring the component -->
    <AdviceExpression AdviceId="urn:siera:example:obligation:log-access:file" AppliesTo="Permit">
        <AttributeAssignmentExpression AttributeId="urn:siera:example:obligation:log-access:file:path">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                /var/log/siera/file.log
            </AttributeValue>
        </AttributeAssignmentExpression>
    </AdviceExpression>
</AdviceExpressions>
```

Figure 27. Extrait d'une règle XACML - partie Obligation/Conseil

La validité de ce travail a aussi été démontrée au travers de l'évaluation des performances de notre prototype. Le test a consisté à l'envoi d'une requête qui peut amener à deux décisions : 1) Soit le PDP accepte la requête sans obligation, 2) soit il accepte la requête mais la décision comporte aussi une obligation qui consiste à enregistrer dans un fichier de log une chaîne de caractères (exemple donné dans l'HDR). Chaque test a été exécuté 200 fois afin de calculer le temps moyen, minimum et maximum. Les temps sont donnés en millisecondes. Le prototype utilise l'implémentation Balana d'XACML v3 (Balana XACML 2016). La procédure analysée dans chaque test a été (Figure 28):

- **Test1 : Décision avec obligation (module non installé)**
    1. Envoi requête
    2. Prise de décision et réception de la décision
    3. Analyse de l'obligation et de la recommandation
    4. Copie du fichier module OSGi qui implémente l'obligation (cette copie est locale)
    5. Installation et chargement dans l'environnement OSGi du module
    6. Exécution de l'obligation (écriture dans le fichier)

- **Test 2 : Décision avec obligation (module déjà présent)**
    1. Envoi requête
    2. Prise de décision et réception de la décision
    3. Analyse obligation et recommandation
    4. Exécution de l'obligation (écriture dans le fichier)

- **Test 3 : Décision sans obligation**
    1. Envoi requête
    2. Prise de décision et réception de la décision

	Décision avec obligation (module non installé)	Décision avec obligation (module déjà présent)	Décision sans obligation
Temps moyen	28,0	4,9	3,2
Temps min	25,7	2,7	1,7
Temps max	31,7	16,1	13,8

Figure 28. Performance PEP adaptable - Temps pour chaque test en millisecondes

La définition de (Chung et al. 2004) montre que l'approche d'adaptation utilisée pour le PEP est similaire à celle des politiques auto-contenues. Les conseils inclus dans les réponses du PDP définissent Δ_S. L'administrateur lorsqu'il/elle utilise des obligations dans sa politique, provoque un possible changement d'environnement sur le PEP (fonction *EnvChangeRecognition* : $E' \times E \rightarrow \Delta_E$). Lorsqu'il/elle choisit les composants pour mettre en œuvre les obligations, il/elle décide de la stratégie d'adaptation (fonction *SysChangeRecognition* : $\Delta_E \times S \rightarrow \Delta_S$). Ainsi, le PEP peut réaliser la fonction *SysChange* : $\Delta_S \times S \rightarrow S'$, où meet(S', need(E')). Cependant, contrairement aux politiques auto-contenues qui contiennent Δ_S, les conseils décrivent Δ_S. Nous avons fait ce choix pour ne pas surcharger le réseau avec les composants obligations qui seraient envoyés à chaque réponse XACML.

3.5 Bilan

Ce chapitre a présenté nos travaux sur l'adaptabilité des systèmes de gestion à base de politiques. Ces travaux ont traité des aspects de prises de décisions et de mise en œuvre des politiques de sécurité (Figure 29). Ils ont fait l'objet d'études avec un objectif pratique, c'est à dire que des réalisations concrètes valident les concepts proposés. L'approche suivie a consisté à avancer petit à petit en prototypant à chaque fois les idées proposées. Si je n'ai présenté que les derniers travaux obtenus, de nombreuses étapes ont été nécessaires pour analyser les besoins d'adaptation des architecture à base de politiques (Laborde et al. 2008; Laborde, Cheaito, et al. 2009; Cheaito et al. 2009). Les réalisations ont été effectuées sur des implémentations du standard XACML car nous utilisons cette technologie dans le cadre de nos recherches sur la gestion des accès et des identités. Cependant, nos concepts sont valides de manière plus générale pour les systèmes de gestion basés sur des politiques ABAC. La capacité d'extension d'un langage est aujourd'hui nécessaire pour pouvoir s'adapter aux nouveaux besoins métiers. Nos travaux ont montré comment adapter dynamiquement un système de gestion pour qu'il puisse interpréter et mettre en œuvre les extensions du langage.

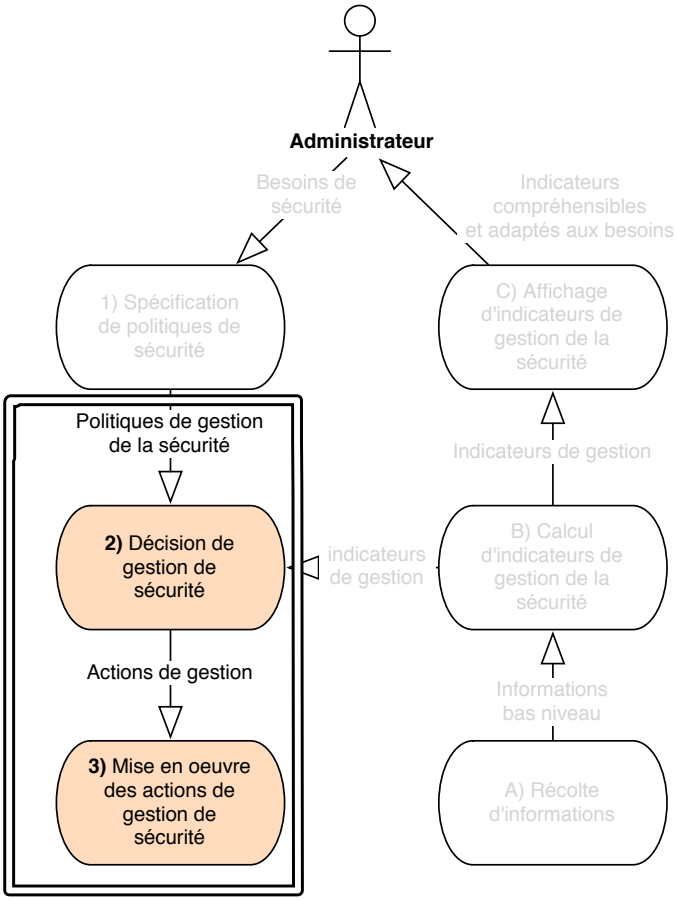


Figure 29. Eléments de la boucle de gestion traités dans le chapitre 3

Aujourd'hui, nos résultats sur l'adaptabilité des entités de gestions nous permettent de concevoir des entités de gestion que nous pouvons modifier au besoin et ce dynamiquement. Cependant, une seule adaptation Δ_S est spécifiée. Il faudrait étendre ces travaux à plusieurs adaptations possibles qui dépendraient du contexte ou de la situation de gestion. Par exemple, une information de gestion peut être capturée par un PEP ou par un PIP au niveau du PDP. De même, une même obligation peut être mise en œuvre différemment selon le PEP ou une condition. Il serait intéressant de pouvoir adapter cette mise en œuvre. Il existe des travaux très intéressants sur le déploiement de logiciel autonome (Arcangeli et al. 2015) où des solutions ont été proposées pour gérer automatiquement le cycle de vie du déploiement d'un logiciel distribué et ce selon différents critères.

Sur le plan expression, il existe aussi des travaux intéressants sur l'expression de règles génériques en XML avec l'initiative RuleML (« RuleML Wiki » 2015). Cependant, on peut se poser la question sur la pertinence d'utiliser des langages basés sur XML ou JSON pour exprimer les politiques de sécurité du futur. Par exemple, initialement, XML a été défini pour 1) stocker et transporter des données, 2) être à la fois lisible par un être humain et une machine (W3 Schools 2015). Ce choix était judicieux lorsque l'on devait représenter des configurations d'équipements. Or les politiques que l'on exprime en XACML sont de moins en moins des données et de plus en plus des programmes qui contrôlent le système géré ; en particulier avec l'utilisation des obligations. Ainsi, nos travaux sur

l'adaptation des PEPs qui permettent de charger des modules OSGi peuvent aussi être vus comme la construction d'un interpréteur de code écrit en XML. Enfin, ma deuxième remarque porte sur la lisibilité d'un « code de politique de sécurité » écrit en XML. Les politiques étant de plus en plus complexes, la lisibilité d'une politique de sécurité complexe écrite en XACML est plus que contestable malgré différents efforts comme (Stepien et al. 2014; Nergaard et al. 2015).

Chapitre 4. Analyse de configurations de sécurité réseau

Ces travaux ont été traités dans le cadre de la thèse de Hicham El Khoury (El Khoury 2014).

4.1 Présentation de la problématique

La sécurité des applications distribuées est supportée par un ensemble de services de sécurité réseau. Les services de sécurité aujourd'hui reconnus sont ceux définis par l'ISO (ISO 7498-2 1989) (le contrôle d'accès, l'identification/authentification, la confidentialité, l'intégrité et la non répudiation) auxquels on ajoute la traçabilité. Ces services de sécurité sont implémentés au moyen de mécanismes de sécurité comme les protocoles (IPSec, L2TP, SSL, SSH, PPPoE, …) ou encore de mécanismes de contrôle d'accès (les pare-feux, les Application Level Gateways, les contrôles d'accès sur les systèmes).

Par nature, la gestion de la sécurité pour des applications réparties est une fonction distribuée qui implique la coordination d'un ensemble d'équipements possédant chacun des capacités et des services de sécurité spécifiques. Ainsi, tout équipement (terminal ou intermédiaire) impliqué dans la sécurité requiert une configuration précise. Cette configuration, déterminant le comportement de l'équipement, a un impact local à l'équipement sur la sécurité définie. Toutefois, chacune des règles de configuration a aussi un impact sur la sécurité globale du réseau. Si une règle sur un équipement est mal définie, le principe du maillon le plus faible de la chaîne s'appliquant, la sécurité globale peut être compromise. Ainsi, le niveau de protection correspond à la combinaison de plusieurs technologies qui doivent être installées sur plusieurs équipements, chacun de ces derniers ayant sa propre configuration. Il faut donc contrôler la cohérence et le niveau de sécurité globale des composants interconnectés.

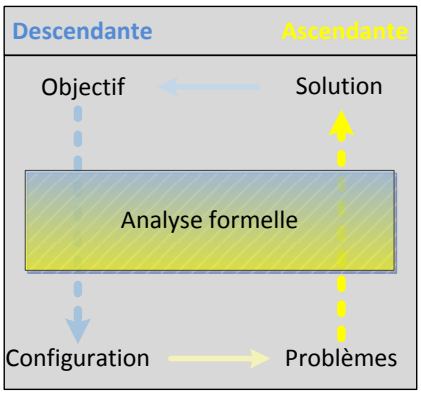


Figure 30. Analyse de configurations de sécurité réseau

Cette problématique intervient dans deux processus (Figure 30) :

- Approche Descendante : Cette approche, appelée aussi raffinement, consiste à utiliser différents niveaux d'abstraction de l'information de gestion afin traduire des exigences de sécurité en configurations.
- Approche Ascendante : Cette approche est utilisée pour diagnostiquer un mauvais fonctionnement des équipements réseaux. Elle consiste à analyser les configurations existantes sur les équipements de sécurité et en déduire l'origine du problème.

Dans les deux cas, face à l'innombrable quantité de protocoles implémentés, de mécanismes de sécurité déployés et configurables par de multiples paramètres, comment s'assurer qu'une configuration est non-conflictuelle avec les autres configurations et correcte par rapport à la politique de sécurité ?

Ajouté à cela, bien que des mécanismes puissent paraître similaires par leurs noms ou le service de sécurité offert, leurs composants internes peuvent être différents (e.g., un pare-feu Cisco, une machine Linux avec iptables ou ipchains sont tous des pare-feux mais ils n'ont pas exactement les mêmes mécanismes). Ainsi, si nous désirons analyser des configurations de sécurité réseau nous devons nous poser aussi la question suivante : Comment peut-on représenter ces mécanismes de manière générique?

4.2 Quelques travaux connexes

Une inconsistance peut apparaître lorsque deux règles d'un même mécanisme sur un même équipement sont incompatibles. Par exemple, un pare-feu possède deux règles de filtrages telles que l'une accepte tous les flux de données avec comme adresse IP source 10.0.0.0/8 et l'autre bloque certains flux de données avec pour adresse IP source 10.20.30.40. Nous appelons cela inconsistance atomique (Laborde et al. 2005). La manière la plus simple de résoudre de tels conflits consiste à mettre œuvre un algorithme particulier qui amènera à une décision unique de la part de l'équipement de sécurité configuré telle que la première règle trouvée est celle qui sera appliquée (Samarati et al. 2001). Si ces algorithmes résolvent les conflits et donc garantissent que l'équipement n'aura qu'une unique règle à appliquer, ils ne permettent pas l'analyse et la détection à-priori des inconsistances. Ils ne garantissent pas la cohérence des règles qui seront appliquées. Ils ne s'appliquent pas non plus à ce que nous appelons l'inconsistance distribuée (Laborde et al. 2005), c'est à dire l'incompatibilité de deux règles/configurations entre des mécanismes différents sur des équipements différents. Par exemple, lorsqu'un tunnel IPsec entre deux routeurs IPsec est « coupé » par un pare-feu intermédiaire.

Des recherches ont été menées pour répondre à ces problèmes en focalisant d'abord sur les pare-feux. Al-Shaer et Hamed ont proposé la première taxonomie permettant de classifier les différentes anomalies entre règles de pare-feu sans état (Al-Shaer et al. 2004). En se basant sur une représentation des règles de pare-feu, ils ont défini des relations entre règles de filtrages telles que l'inclusion,

l'équivalence, la disjonction complète et partielle, ou encore la corrélation. Ces relations sont ensuite utilisées pour définir des types d'anomalies. Des algorithmes ont été proposés permettant de détecter ces anomalies mais de proposer des corrections (Al-Shaer et al. 2005). Cuppens et al. (Cuppens et al. 2015) ont généralisé la modélisation des règles de filtrage qui était limitée aux adresses IP, aux numéros de ports et au protocole encapsulé. (Basile et al. 2004) ont développé la notion d'interprétation géométrique d'une politique de filtrage et ont proposé des algorithmes pour la découverte d'anomalies dans un pare-feu stateless, ainsi que lors de l'insertion (la mise à jour) de nouvelles règles. Les parefeux stateless ayant tendance à être remplacés par des pare-feux stateful, des travaux plus récents ont tenté de détecter les anomalies en prenant en compte l'état d'une connexion comme (Gouda et al. 2005), (Buttyán et al. 2009) ou (Cuppens et al. 2012).

Plusieurs mécanismes de sécurité concourent à la protection d'un réseau, il est donc nécessaire de considérer ces différents équipements dans l'analyse de la mise en œuvre d'une politique de sécurité. Les travaux de Fu et al. (Fu et al. 2001) exposent la nécessité d'un système de gestion pour assurer un service de sécurité de bout-en-bout en considérant deux mécanismes : le filtrage et les VPN IPsec. Ils introduisent deux niveaux pour spécifier une politique de VPN IPSec : un niveau « haut » qui représente et analyse les objectifs de la politique IPsec et un niveau « bas », correspond à l'implémentation de la politique dans les composants de sécurité. Ils ont développé des mécanismes pour détecter et résoudre les conflits entre les stratégies IPSec pour assurer des communications sécurisées de bout en bout. Al-Shaer et al. (Hamed et al. 2006) ont repris leur précédent travail sur les anomalies de configuration de pare-feu (Al-Shaer et al. 2004) et ont produit une classification des anomalies pouvant affecter les configurations IPSec.

D'autres travaux ont analysé à la fois la consistance et l'exactitude des règles de configurations de plusieurs types d'équipements. Une approche formelle basée sur les flux de données a été proposée par Guttman et Herzog (Guttman et al. 2005). Le but de cette approche est de déterminer si une configuration du réseau incluant des pare-feux et des passerelles IPsec vérifie bien les objectifs de sécurité. En parallèle, durant ma thèse (Laborde et al. 2005; Laborde et al. 2007) j'ai proposé une approche de raffinement de politique en se basant sur le formalisme des réseaux de Petri colorés (Jensen 1987) incluant une modélisation des réseaux orientée flux de données mais où les traitements sur les flux de données sont plus abstraits. En réutilisant la modélisation de réseau de (Guttman et al. 2005), Uribe et Cheung (Uribe et al. 2004) ont développé un outil de spécification et de vérification pour les réseaux qui comportent plusieurs pare-feux et plusieurs IDS. Dans (Al-Shaer et al. 2009), les auteurs ont proposé une nouvelle approche nommée « ConfigChecker » qui permet de modéliser le réseau comme une machine à états finis où chaque état du réseau est déterminé par les datagrammes IP dans le réseau. Preda et al. (Preda et al. 2010) ont proposé un processus de raffinement. Partant des règles d'autorisation concrètes OrBAC (Kalam et al. 2003), ils en déduisent des configurations de pare-feu, de VPN IPsec et de système de détection d'intrusion en utilisant la méthode B classique

(Abrial et al. 2005). Plus tard, les travaux issus de (Preda et al. 2010) et (Alfaro et al. 2008) ont été implémentés dans MIRAGE (Garcia-Alfaro et al. 2011) pour garantir l'exactitude et la consistance des règles de configuration des politiques de sécurité réseau simples et distribués. Il met en œuvre une analyse des configurations de composants de pare-feu, routeurs NIDS, et VPN pour détecter les anomalies lors du déploiement.

Les travaux axant la modélisation sur les configurations des équipements ont développés des algorithmes qui sont très liés à la sémantique des éléments de configuration. En conséquence, les modèles proposés sont liés à une ou plusieurs technologies précises et il est très difficile de les adapter à de nouvelles technologies. Lors de ma thèse j'avais suivi une autre voie orientée flux de données pour palier ce problème. A la vue des travaux plus récents, d'autres chercheurs sont arrivés à la même conclusion. Cependant, les modélisations des flux de données sont encore assez basiques car limités au datagramme IP et quelques champs du protocole transport (Guttman et al. 2005; Uribe et al. 2004; Al-Shaer et al. 2009; Preda et al. 2010). Or 1) aujourd'hui, les mécanismes de sécurité travaillent à différents niveaux du modèle OSI, 2) dans le futur il y aura de nouveaux protocoles à considérer, et 3) la pratique actuelle des réseaux consiste à encapsuler les protocoles les uns dans les autres. Nos travaux récents se sont donc tournés vers cette problématique.

L'approche de nos travaux actuels étant fortement inspirés par mes travaux de thèse. Je les présente de manière un peu plus détaillée dans la section suivante.

4.3 L'historique : Mes travaux de thèse

Lors de ma thèse, j'avais proposé une approche de raffinement de politique (Laborde et al. 2007). Déjà à cette époque, je voulais que mon approche soit indépendante des technologies. Je m'étais rendu compte que la meilleure façon d'y arriver était de travailler sur les flux de données. Par conséquent, j'avais défini le flux de données comme élément central dans mon approche de raffinement.

Mon processus de raffinement est découpé en trois phases (Figure 31). L'expression des objectifs de sécurité réseaux qui sont déterminés à partir de politique de contrôle d'accès RBAC. La définition d'une tactique de sécurité qui est une représentation abstraite d'une solution pour mettre en œuvre les objectifs de sécurité. Une tactique de sécurité est indépendante de la technologie. La validation d'une tactique consiste à analyser sa consistance (pas de règles contradictoires) et son exactitude (représente-t-elle l'objectif de sécurité). Enfin, les configurations de sécurité qui représentent la mise en œuvre d'une tactique dans un environnement technologique cible. Le processus valide si une tactique peut effectivement être mise en œuvre dans un environnement donné.

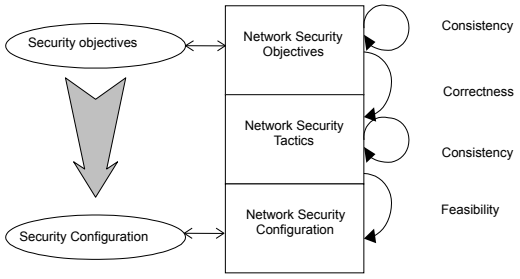


Figure 31. Processus de raffinement durant ma thèse

L'approche de modélisation consiste à déterminer les fonctionnalités de base dans la sécurité des réseaux qui lorsqu'elles sont combinées permettent de spécifier n'importe quel type d'équipement. Un flux de données peut être produit/consommé, propagé, transformé ou filtré indépendamment des technologies utilisées. Notre choix permet de limiter le nombre de cas à prendre en compte et donc de simplifier la spécification des tactiques de sécurité. Par conséquent, nous représentons un équipement non pas comme une entité propre mais par les traitements qu'il est capable d'appliquer sur les flux de données. Nous avons isolé quatre fonctionnalités de base (Figure 32) :

- Les fonctionnalités qui *produisent* ou *consomment* les flux de données comme les systèmes terminaux sont appelées des **terminaisons de flux** (EF pour End-Flow). Elles définissent le périmètre d'une structure de communication ; cela peut être un équipement terminal (par exemple un PC ou un équipement serveur), comme un processus applicatif (par exemple une application cliente ou serveur). Elles sont connectées aux entités sujets/objets du modèle RBAC. Une EF qui est associée à une entité active du modèle de niveau application (les utilisateurs dans le modèle RBAC), est appelée terminaison de flux active (AEF - Active End-Flow). Une EF qui est associée à une entité passive du modèle de niveau applicatif (les objets dans le modèle RBAC) est appelée terminaison de flux passive (PEF - Passive End-Flow). Les flux produits dépendent des permissions assignées aux rôles des sujets. Un ensemble de rôles est associé à chaque EF. Les rôles d'une EF proviennent des rôles de l'entité de niveau application qui est connectée. Un rôle associé à une EF représente ici simplement une abstraction des flux de données que l'EF peut produire et donc implicitement les objectifs de sécurité réseaux. Un flux est défini par *(efs, efd,rôle, liste_transf)* où *efs* est l'EF émettrice, *efd* est destinataire, *rôle* est le rôle caractérisant le flux de données, et *liste_transf* est la liste des transformations appliquées au flux de données.

- Les fonctionnalités qui *propagent* les flux de données comme les supports de communication sont appelées des **fonctionnalités canal**. Les fonctionnalités canal représentent les environnements de propagation des flux de données qui peuvent être physique (bus de communication d'un ordinateur, câble, air pour le WIFI) ou une abstraction pour les systèmes non connus (Internet).

- Les fonctionnalités qui *transforment* les flux de données où l'on retrouve les protocoles de sécurité sont appelées des **transformations**. Les fonctionnalités de transformation représentent la capacité de modifier un flux de données. Cela peut être un protocole de chiffrement comme IPsec où une fonctionnalité transforme un flux de données en y ajoutant un service de sécurité (par exemple la confidentialité) et une autre fonctionnalité enlève cette transformation. Cela peut être également le NAT en quel cas une seule fonctionnalité de transformation est impliquée et aucun service de sécurité n'est ajouté au flux de données. Les règles de transformations sont de la forme $\{ef_s\},\{ef_d\},$rôle → groupe où $\{ef_s\}$ désigne l'ensemble des terminaisons de flux sources, $\{ef_d\}$ l'ensemble des terminaisons de flux destinations, *rôle* le rôle utilisé pour envoyer ce flux de données et *groupe* la transformation à effectuer

- Les fonctionnalités qui *filtrent* les flux de données comme les pare-feux sont appelées des **filtres**. Les fonctionnalités de filtre représentent la capacité de bloquer ou de laisser passer un flux de données. Elles représentent le service de contrôle d'accès. Il peut se situer à différents niveaux : les modules de contrôle d'accès des systèmes d'exploitation, les serveurs mandataires, les pare-feux, ou encore le contrôle d'accès sur les commutateurs. Une règle d'une fonctionnalité de filtrage est un ensemble de 4-tuples de la forme *{efs},{efd},rôle,groupe* où $\{ef_s\}$ désigne l'ensemble des terminaisons de flux sources, $\{ef_d\}$ l'ensemble des terminaisons de flux destinations, *rôle* le rôle utilisé pour envoyer ce flux de données et *groupe* le dernier groupe de transformation appliqué.

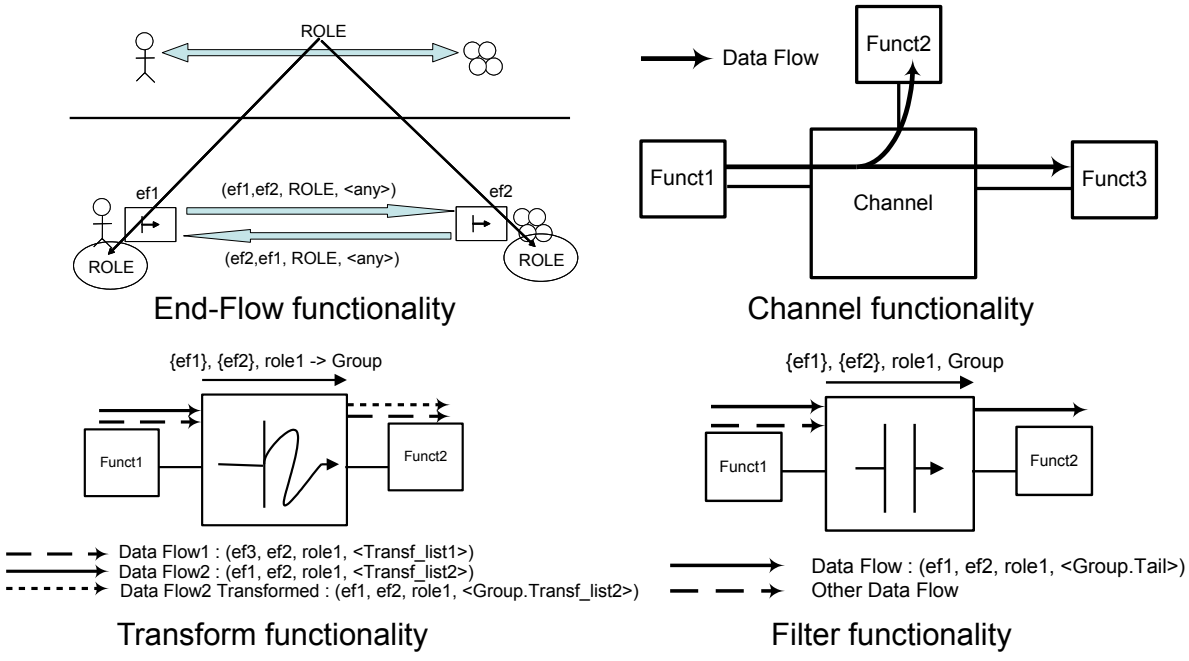


Figure 32. Fonctionnalités permettant de décrire les traitements sur un flux de données

Chaque fonctionnalité a été spécifiée dans le formalisme des réseaux de Petri colorés (CPNs). De plus, j'avais démontré que toute tactique de sécurité donne un CPN K-borné, et donc que le nombre d'états générés est borné. Cela permettait de pouvoir analyser les états du CPN avec des approches de model checking. De plus, les modèles CPN des fonctionnalités ont été créés de telle manière que le graphe d'états n'ait qu'un seul état puis et que celui-ci soit nécessaire et suffisant pour analyser le modèle. Ainsi, une simple simulation permet d'atteindre l'état puits et valider une tactique par rapport aux propriétés suivantes:

- *Propriété de confidentialité* : La propriété de confidentialité prévient de la divulgation non autorisée d'information. Dans cette modélisation, elle est exprimée par le fait que les terminaisons de flux actives ne doivent à aucun moment recevoir des flux de données lisibles avec des rôles qui ne leur ont pas été assignés.
- *Propriété d'accessibilité* : Toutes les terminaisons de flux actives (resp. passives) doivent pouvoir consommer les flux de données pour tous les rôles qui leur sont assignés provenant de toutes les terminaisons de flux passives (resp. actives) assignées à ces mêmes rôles.
- *Propriété de cloisonnement* : Un flux de données ne peut traverser un réseau que si ce dernier se trouve entre la source et la destination autorisées. Ainsi, une fonctionnalité de filtre ne doit laisser passer un flux de données que lorsqu'elle se trouve entre une source et une destination autorisées pour ce flux de données.
- *Règles de transformation et de filtrage non productives* : Une règle de filtrage ou de transformation est dite non productive si elle n'est jamais utilisée par une fonctionnalité de filtrage ou de transformation.

Modéliser des équipements configurés par rapport au traitement qu'ils effectuent sur les flux de données a montré ses avantages. Le formalisme utilisé permet une approche indépendante des technologies. Cependant, je me suis rendu compte que le niveau d'abstraction de la modélisation des flux (un flux est vu comme *(efs, efd, rôle, liste_transf)*) est trop élevé et ne permet pas de représenter explicitement ce qui a été modifié par une transformation. J'avais dû ajouter dans mon approche de raffinement une étape pour vérifier la faisabilité d'une stratégie de sécurité sur un système réel. Nos travaux actuels se situent dans le même cadre de raffinement, mais tentent de mieux capturer la notion de flux de données.

4.4 Une nouvelle formalisation orientée flux de données

La modélisation des flux de données par nos précédents travaux étant limités, nous nous sommes alors poser les questions suivantes :

- Comment modéliser un flux d'une manière générique ?
- Comment manipuler ce flux de données d'une manière unifiée ?

- Comment modéliser un mécanisme avec sa configuration pouvant manipuler ces flux de données ?

4.4.1 Un modèle formel de flux de données

Nous sommes partis de la constatation qu'un message envoyé sur le réseau était une encapsulation de protocoles. Plus précisément, un flux de données réel peut être vu comme un ensemble contigu ou non d'octets de taille variable véhiculé sur un réseau. Cette suite d'octets est décomposée en blocs logiques respectant une encapsulation de protocoles notée par « $\mathcal{E}$ ». Par exemple, un flux de données correspondant à une requête HTTP peut être vu comme <bloc protocole Ethernet, bloc protocole IP, bloc protocole TCP, bloc protocole, bloc protocole HTTP>. Chaque protocole divise le bloc d'octets associé en champs, que nous appelons attributs, selon sa description. Par exemple, les informations de contrôle du protocole Ethernet sont réparties en 14 octets (adresse MAC destination, adresse MAC source, identifiant du protocole encapsulé) au début de la trame et 4 octets pour le champ de contrôle à la fin. Modéliser un flux en terme d'attributs permet à la fois de représenter fidèlement un flux de données réel ou même d'utiliser des abstractions selon les besoins. Ces éléments ont été représentés ainsi :

- $\boldsymbol{\mathcal{A}}$ est l'ensemble des attributs possibles. Un attribut $a \in \mathcal{A}$ est un couple <name, value> tel que *name* est un champ quelconque que l'on peut trouver dans un protocole et *value* est son contenu,
- $\boldsymbol{\mathcal{P}}$ est l'ensemble des protocoles, c'est à dire l'ensemble des blocs logiques protocole. Ainsi un protocole $p \in \mathcal{P}$ est vu comme un couple <protoid, attributes> tel que protoid=<name, id> contient le nom du protocole *name*, son identifiant unique *id* et *attributes* est l'ensemble des attributs de p et est défini sur l'ensemble des parties de $\mathcal{A}$, i. e. , $\text{attributes} \in \mathbb{P}(\mathcal{A})$,
- $\boldsymbol{\mathcal{E}} = \mathcal{P}^{\mathbb{N}}$ est l'ensemble des séquences finies sur $\mathcal{P}$. Cet ensemble représente l'ensemble des chaînes d'encapsulation de protocoles, i.e. des séquences de blocs logiques protocoles,

Dans un objectif d'analyse, il est nécessaire de garder l'historique des traitements effectués sur une chaîne d'encapsulation de protocoles (par exemple, application de DES, 3DES, HMAC-SHA1, etc) et le niveau de chiffrement. Pour cela, nous avons associé à l'encapsulation de protocoles deux ensembles (AUTHN et CONF) qui représentent les attributs du flux de données ayant été authentifiés et chiffrés respectivement. Par exemple, si le traitement consiste en l'utilisation d'IPsec ESP, cela revient à ajouter de nouveaux protocoles dans la chaîne d'encapsulation ainsi que de nouvelles instances dans l'ensemble AUTHN et le multi-ensemble CONF. Pour prendre en compte les techniques de chiffrement, nous définissons :

- $\mathcal{S}$ est l'ensemble des algorithmes de sécurité traitant les chaînes d'encapsulation de protocoles (par exemple, DES, 3DES, HMAC-SHA1, etc).
- $\mathcal{L}$ ={all,val} représente le niveau de chiffrement d'un attribut. La valeur *all* indique qu'il impossible de déterminer où se trouve l'attribut dans le flux. Par exemple, lors de l'utilisation ESP (Kent 2005), l'emplacement des champs des protocoles protégés par ESP ne peuvent être déterminés. Par contre, d'autres mécanismes comme XML-Encryption (XMLENC 2002) permettent de chiffrer soit tout un bloc XML soit uniquement un élément du bloc XML. Dans ce dernier cas, il est possible de déterminer l'emplacement de l'attribut contrairement au cas ESP, mais il est normalement impossible de connaître sa valeur sauf si la clé secrète est connue. Pour modéliser cette possibilité nous utilisons la valeur *val* qui indique que l'emplacement de l'attribut peut être déterminé mais pas sa valeur sauf si la clé est connue.

A partir de ces éléments, nous avons défini l'ensemble des flux de données (El Khoury et al. 2011) par : $\mathcal{F} \subseteq \mathcal{E} \times \text{AUTHN} \times \text{CONF}$

où :

- $\mathcal{E}$ est l'ensemble des chaînes d'encapsulation,
- $\mathbf{AUTHN} \subseteq (\mathcal{A} \times \mathcal{P} \times \mathcal{A} \times \mathcal{P} \times \mathcal{S})$ représente les attributs du flux de données qui ont été authentifiés tel que $(a_1, p_1, a_2, p_2, s) \in \text{AUTHN}$ indique que l'attribut a_1 du protocole p_1 garantit l'intégrité de l'attribut a_2 du protocole p_2 via l'algorithme de sécurité s,
- $\mathbf{CONF} \subseteq \text{BAG}(\mathcal{A} \times \mathcal{P} \times \mathcal{S} \times \mathcal{L})$ représente les attributs du flux de données qui ont été chiffrés, tel que :
  - $(a, p, s, \text{all}) \in \text{CONF}$ indique que l'attribut a du protocole p est complètement chiffré par l'algorithme de sécurité s et
  - $(a, p, s, \text{val}) \in \text{CONF}$ indique que seule la valeur de l'attribut a du protocole p est chiffré par l'algorithme de sécurité s.

4.4.2 Représentation des mécanismes de sécurité basée sur les flux de données

Un traitement sur un flux de données est alors vu comme une fonction particulière de $\mathcal{F}$ dans $\mathcal{F}$. Chaque traitement selon la technologie utilisée considère un ensemble d'attributs du flux de données en entrée (par exemple les attributs adresses IP source et destination et protocole transport du protocole IP et les attributs numéros de port source et destination du protocole TCP/UDP pour une passerelle IPsec) et peut être bloqué, propagé, transformé ou filtré indépendamment des technologies utilisées. Nous avons défini formellement neufs fonctions élémentaires pour manipuler un flux de données (deux fonctions pour l'extraction d'information qui s'appliquent sur les protocoles et les

attributs, et sept fonctions qui permettent la modification du contenu d'un flux). Ainsi, la spécification du traitement effectué par un équipement est une combinaison particulière de fonctions élémentaires. Cette spécification représente la capacité de traitement de l'équipement sur les flux de données. La capacité définit ce que l'équipement peut potentiellement faire. Par exemple, un pare-feu peut filtrer les datagrammes en analysant les adresses IP, les champs ports, … manipulés grâce à certaines expressions (e.g., égalité entre adresses IP, appartenance à un réseau IP, etc.) Un proxy HTTP peut modifier les messages HTTP en analysant un ensemble de champs HTTP. Le traitement effectivement effectué par un mécanisme particulier dépend aussi d'une configuration donnée. La configuration définit un comportement spécifique basé sur la capacité du mécanisme. Par exemple, la configuration d'un mécanisme pare-feu va indiquer que « si adresse IP source appartient à 1.0.0.0/8 alors bloquer ». Ceci correspond donc à un comportement particulier créé par rapport à la capacité de traitement du mécanisme. En conséquence, nous définissons un mécanisme « M » par $CAPABILITY_M$ pour représenter la capacité spécifique et par $CONFIGURATION_M$ pour représenter une configuration spécifique pour un mécanisme spécifique (El Khoury et al. 2012) :

$$\mathbf{M} = < \mathbf{CAPABILITY_M}, \mathbf{CONFIGURATION_M} >$$

$\mathbf{CAPABILITY_M} = < \mathbf{\Sigma_M}, \mathbf{A_M}, \mathbf{EXPR_M^A} >$ est la capacité potentielle du mécanisme M avec :

1) $\boldsymbol{\Sigma_M}$ est l'ensemble fini non vide de types de données reconnus par M,

2) $\boldsymbol{A_M} = \boldsymbol{A_M^F} \cup \boldsymbol{A_M^{ctx}}$ | $A_M \subseteq \mathcal{A}$ et $\forall$ $a_i \in A_M$, $Type(a_i) \in \Sigma_M$; A_M^F est l'ensemble des attributs d'un flux de données F qui peuvent être récupérés par le mécanisme M, et A_M^{ctx} est l'ensemble des attributs de contexte trouvé dans une règle de configuration. Nous appelons « attributs de contexte », les attributs ne sont pas trouvés dans le flux de données (e.g., la mémoire d'états des pare-feux),

3) $\boldsymbol{EXPR_M^A}$ est l'ensemble fini des expressions évaluables par M et portant sur des variables libres appartenant à A_M.

Nous définissons les éléments de configuration d'un mécanisme M par une liste de règles « $RULE_M^A$ » et un algorithme de résolution des conflits « CRA » où tous les deux sont basés sur un ou plusieurs éléments de la capacité du mécanisme « $CAPABILITY_M$ » :

$$\mathbf{CONFIGURATION_M} \in \mathbf{RULES_M} \times \mathbf{CRA_M}$$

Une règle d'un mécanisme M consiste en un ensemble de contraintes sur des attributs A_M, conjointement avec un ensemble d'actions $ACTION_M$:

$$\mathbf{RULE_M^A} \subseteq \mathbf{CONDITION_M^A} \times \boldsymbol{ACTION_M^A}$$

Les actions sont les traitements disponibles implantés sur le mécanisme. Ces actions sont exprimées au moyen des fonctions élémentaires de manipulation de flux de données que nous avons définies (El–Khoury et al. 2014).

4.4.3 Analyse des configurations des mécanismes de sécurité réseau

Nous avons exprimé notre modèle dans le langage des CPNs hiérarchiques afin de valider notre approche et d'utiliser les outils d'analyse associés implantés dans le logiciel « CPN Tools » (« CPN Tools » 2015). Nous avons défini un modèle CPN appelé GAM (pour Generic Attribute-based Mechanism model) comme bloc logique de base d'un mécanisme de sécurité réseau. Une technologie de sécurité est alors représentée par un GAM ou une combinaison de GAMs.

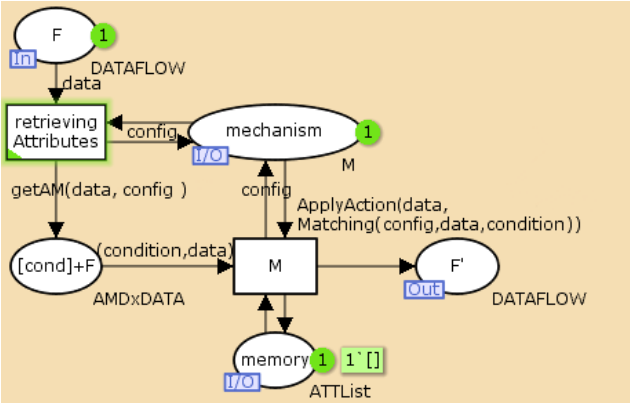


Figure 33. Présentation de GAM en CPN

Un GAM prend en entrée un flux de données (place F dans la Figure 1 marqué par « In » en bleu) et retourne un flux de données comme sortie (place F' dans la Figure 1 marqué par « Out » en bleu). La description de ce mécanisme générique est définie dans la place « mechanism » qui contient la capacité et la configuration de ce mécanisme. Finalement, les attributs contextuels trouvés dans une règle de configuration du mécanisme M « A_M^{ctx} » sont stockés dans la place « mémoire ». Cette mémoire, par la suite, peut être utilisée pour représenter des mécanismes à état. En outre, le lieu «mémoire» peut être partagé par différents mécanismes génériques. Nous nous sommes inspirés de l'architecture gestion à base de politique pour exprimer ce GAM.

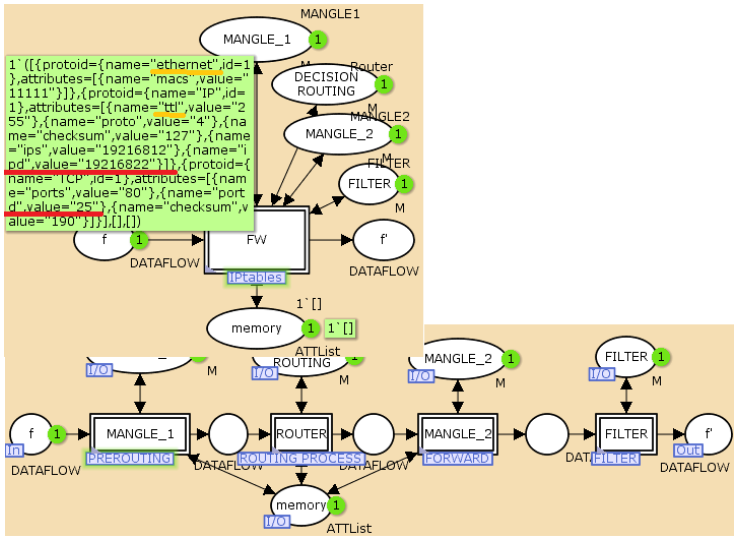


Figure 34. Exemple de spécification d'IPtables

Un GAM une structure est générique. Pour qu'il représente un mécanisme particulier, il faut le spécialiser en définissant sa capacité et sa configuration. Dans le formalisme des CPNs, cette spécialisation consiste uniquement à définir un jeton décrivant sa capacité et sa configuration dans la place « mechanism ». Un GAM avec une capacité d'un pare-feu et une configuration sera un mécanisme de pare-feu configuré. Un GAM avec une capacité IPsec et une configuration sera une passerelle IPsec.

Ainsi, une spécification d'un réseau consiste alors à interconnecter des GAMs entre eux en définissant à chaque fois la capacité et la configuration. De plus, grâce aux CPNs hiérarchiques, il est possible de créer de mécanismes abstraits. L'exemple de la Figure 34 représente une modélisation d'IPtables où le mécanisme FW correspond en fait à la chaîne de traitement Mangle1 -> Router -> Mangle2 ->filter.

Nous avons appliqué notre approche de modélisation sur différentes études de cas : utilisation de IPsec et du NAPT (El–Khoury et al. 2014), ou encore l'analyse fine d'une configuration iptables (El Khoury et al. 2013). Nous avons pu en dégager des éléments d'appréciation quant à la capacité d'expression et d'analyse de notre approche. En particulier, nous avons pu détecter par simulation des conflits de configurations sans nécessiter de connaissances ou d'expérience à priori dans le domaine.

4.5 Bilan

Ce chapitre a présenté nos travaux sur l'analyse de configuration de sécurité réseau. Ils s'inscrivent dans un processus plus global de raffinement de politique de sécurité qui a pour objectif de garantir que la mise en œuvre de politiques de sécurité correspond aux exigences de sécurité (Figure 35). Ces travaux ont plutôt été théoriques. Toutefois, nous avons toujours cherché à appliquer notre travail à des cas concrets. Il est intéressant de noter que l'inspiration de notre modèle orienté flux de données ainsi que le mécanisme générique à base d'attributs (que nous appelons GAM) provient de

notre expérience dans le domaine de la gestion des identités et des accès présenté dans le chapitre 2 (expression à base d'attribut et gestion à base de politique). Nous avons ainsi pu proposer un modèle très flexible. Cependant, un travail important reste à entreprendre sur l'analyse de spécifications. Pour l'instant cette analyse est limitée à de la simulation. Si nous voulons pouvoir utiliser des approches de types model-checking, nous devons prouver que les spécifications générées selon notre approche engendrent des CPN K-bornés comme j'avais pu le faire durant ma thèse. Une des difficultés importante sera le traitement de ce que nous avons appelé les attributs de contexte et des mécanismes stockant en mémoire des informations pour les prises de décisions futures. Ce sujet est aujourd'hui de plus en plus traité en particulier pour l'analyse des pare-feux à états. Par la suite, il faudra aussi inclure ces travaux dans un processus de raffinement complet de l'information de gestion de la sécurité.

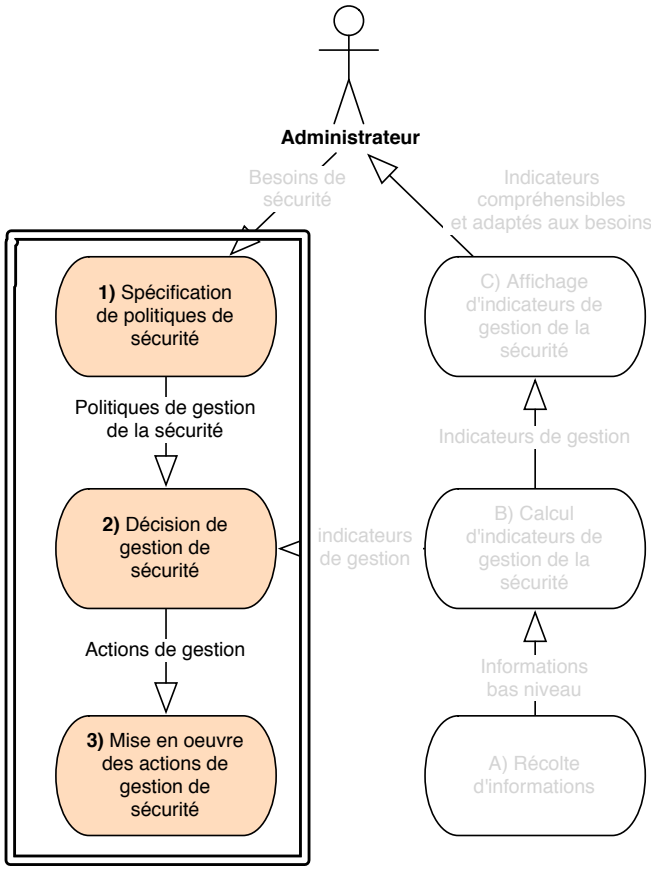


Figure 35. Eléments de la boucle de gestion traités dans le chapitre 4

Un des aspects que je n'ai fait que survoler durant ma thèse et qui m'intéressent de plus en plus est la définition des exigences de sécurité. Comment éliciter des exigences de sécurité ? Comment analyser des exigences de sécurité ? Comment relier ces informations à la fois aux spécifications de sécurité et aux configurations. Cela permettra de s'inscrire dans l'approche dite de « security-by-design » afin de proposer une méthodologie couvrant l'ensemble du processus partant des exigences de sécurité jusqu'aux configurations déployées sur les équipements réseaux. Cette méthodologie doit

offrir un support rigoureux pour garantir une traçabilité entre les exigences de sécurité et les configurations, cela dans l'objectif :

1. D'assurer que les exigences de sécurité sont correctement exprimées et validées,
2. D'assurer que les exigences de sécurité sont bien prises en compte par les configurations des composants du système,
3. De pouvoir déterminer l'impact d'incidents ou d'attaques sur les exigences de sécurité et sur le niveau de criticité des applications métier.

Plusieurs méthodes d'ingénierie des exigences ont été proposées dans la littérature. Les approches utilisant UML ont pour avantages d'utiliser un langage qui est déjà largement répandu et donc de pouvoir s'intégrer facilement dans des approches d'ingénierie classiques utilisant ce langage de modélisation. Toutefois, elles ne possèdent pas de sémantique formelle et donc ne peuvent pas fournir d'outils de validation formelle. L'analyse sécurité est alors effectuée uniquement via l'introduction de menaces (par exemple, mis-use case, abuse case, etc). Les approches d'ingénierie des exigences orientées par les buts (Regev et al. 2005) telles que KAOS (Van Lamsweerde 2009) ou I*/TROPOS (Giorgini et al. 2005) possèdent à la fois un langage graphique et un langage formel. Ainsi ces approches permettent d'analyser les besoins de sécurité par l'introduction de menaces (anti-buts pour KAOS ou menaces pour Secure TROPOS) mais aussi en validant ce qui est exprimé (via des solveurs SAT pour KAOS ou Answer Set Programming pour i*/Secure TROPOS). Néanmoins, ces travaux ont été définis pour la création de logiciels. A notre connaissance, aucune méthode ne traite de la définition des exigences d'une architecture réseau sécurisée.

Chapitre 5. Gestion de la confiance dans les Infrastructures à Clés Publiques

Ces travaux ont été traités dans le cadre de la thèse de Ahmad Samer Wazan (Wazan 2011).

5.1 Présentation de la problématique

Aujourd'hui, l'Internet est le plus large réseau dans le monde. Il permet d'établir des collaborations et est devenu le support de nombre d'interactions que ce soit dans un domaine social ou métier au sens large (comme l'e-commerce) ainsi qu'aux services pour les usagers (comme l'e-administration) équipés de terminaux variés, en s'affranchissant des contraintes spatiales et temporelles.

Si l'utilisation de l'Internet facilite aux usagers l'accès à ces services électroniques (gains en termes de temps, de coût ou encore d'accessibilité), le rapport entretenu par un usager avec un service traditionnel est différent de ce même service dans l'environnement numérique. En effet, il y a deux différences majeures entre les environnements traditionnels et les environnements numériques sur la façon dont la confiance est établie. Tout d'abord, les démonstrations traditionnelles de la confiance que nous avons l'habitude de voir et d'observer dans le monde traditionnel (e.g. les expressions face à face) sont absentes dans les environnements numériques. Ensuite, l'établissement de la confiance passe d'une relation directe dans le monde physique (entre les deux parties de la transaction) à une relation indirecte dans le monde électronique où plusieurs parties dont les deux extrémités de la transaction doivent intervenir pour établir la confiance.

Les utilisations de tierces parties de confiance et de la cryptographie asymétrique font parties aujourd'hui des mécanismes les plus déployés. En particulier, l'usage de deux clés publique et privée (la clé publique peut être échangée librement, et la clé privée doit être cachée) a été mis en œuvre dans les infrastructures à clés publiques (ICP). Dans cette infrastructure, une entité centrale appelée autorité de certification (AC) génère un document électronique (appelé certificat électronique) couplant un nom avec une clé publique et son utilisation possible. Par sa signature, l'AC garantit l'authenticité de ces informations aux entités dépendantes EDs (les entités qui doivent prendre la décision d'accepter ou non un certificat électronique pour une transaction avec le porteur de certificat PdC). L'AC joue donc le rôle de tiers de confiance entre les EDs et les PdCs. Ce modèle à trois entités a été défini dans le standard initial X.509 de 1988 (Figure 36). Depuis, ce standard n'a subi que des modifications mineures telles que l'ajout d'extensions pour aider les EDs à retrouver la politique de certification des

ACs par exemple. Une infrastructure à clés publiques (ICP) est l'organisation qui gère une ou plusieurs ACs.

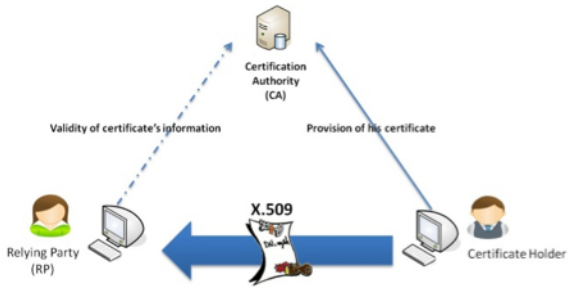


Figure 36. Le modèle de confiance des ICPs X.509 (1988)

L'utilisation de certificats électroniques suivant ce modèle de confiance est aujourd'hui l'un des vecteurs principaux permettant l'établissement de la confiance entre les protagonistes d'une transaction. Dans le contexte de l'e-commerce, les certificats électroniques associés au protocole HTTPS aident les usagers à avoir confiance dans l'identité des serveurs d'e-commerce, mais aussi dans la confidentialité des échanges réalisés lors de la transaction. Nous distinguons deux contextes de déploiement d'ICP. Le *contexte fermé* concerne des communautés d'utilisateurs qui ont des besoins particuliers. Dans ce modèle, toutes les entités finales sont des porteurs de certificats, et les operateurs des ICPs jouent le rôle des entités dépendantes pour la validation des certificats. Les responsabilités et les obligations dans le modèle fermé sont généralement définies en fonction de la relation d'affaires entre les parties. Cela peut être une relation employeur-employé ou une relation contractuelle avec des clients ou des fournisseurs. L'autre contexte, que nous appelons *contexte ouvert*, caractérise un déploiement bien plus large, où tout utilisateur peut potentiellement échanger avec tout autre utilisateur. Ce modèle est celui qui pourrait permettre à n'importe quel utilisateur de pouvoir acheter des marchandises sur n'importe quel site web. Ce modèle est largement ouvert et basé le plus souvent sur un ensemble de règles informelles mises en place par des operateurs privés délivrant des certificats en ligne.

Le modèle de confiance du standard X509 n'est adapté qu'au contexte fermé dans lequel peu d'ACs sont impliquées et où souvent des experts dans le domaine des ICPs aident les EDs (par exemple, l'administrateur sécurité de l'entreprise configure les postes des employés qui des EDs). Dans ce contexte, l'utilisation des certificats est limitée à une application, une collaboration entre organisations possédant chacune leur propre ICP. Les relations entre les différentes entités sont clarifiées au travers de contrats qui s'appliquent à chaque entité. Or l'expert, l'utilisation prédéfinie et les contrats n'existent pas dans un contexte ouvert comme c'est le cas de l'Internet.

Par conséquent, les EDs sont supposées construire leur propre décision de confiance en analysant les documents relatifs aux ACs, i.e., la politique de certificat (CP pour Certificate Policy) et la déclaration des pratiques de certification (CPS pour Certification Policy Statement) si elles veulent répondre à de simples questions telles que : Est-ce que l'identité du PdC a bien été vérifiée ? Que ce passe-t-il si un certificat est faux et que je perds 1000€ parce que je me suis connecté sur un faux site

web ? Est-ce que je suis couvert ? On pourrait argumenter que les navigateurs web font ce travail lorsqu'il indique que tel certificat n'est pas de confiance car l'AC est inconnue. Cependant, le navigateur n'indique pas à quel niveau l'identité du PdC a été vérifiée. Les pratiques des ACs reconnues par les navigateur web sont diverses et variées allant du meilleur au moins bon. L'information fournie à l'utilisateur final est partielle (je ne sais pas si l'AC doit me rembourser mes 1000€). Un navigateur web peut reconnaître une AC alors qu'un autre non. Qui croire ? Enfin, nous avons effectué une étude afin de voir si les navigateurs web validaient correctement les certificats par rapport au standard X.509 (Wazan et al. 2009). Cette étude nous a montré que des certificats valides pouvaient être refusés alors que des certificats non valides étaient acceptés. Ajouté à cela, il n'y a pas que les navigateurs web à considérer. Aujourd'hui, chaque application a sa propre façon d'accepter ou non un certificat pour un utilisateur. Cette situation est complétement ingérable.

Cette complexité qui existe dans le contexte ouvert vient de ce problème de confiance dans les ICPs. Tout d'abord, la gestion de la confiance y est fractionnée ; il existe aujourd'hui un nombre important d'ACs. Au 23 septembre 2015, la liste des ACs reconnues par Mozilla[9] contient 409 certificats dont 182 sont des certificats d'AC auto-signés. En filtrant les champs « organisation » et « pays » du nom des ACs, nous avons pu déterminer qu'il y a 89 ICPs différentes établies dans au moins 30 pays différents (certains noms d'ACs ne contiennent pas le champs indiquant le pays). Un autre exemple de cette complexité est la liste des ACs de confiance de Microsoft mise à jour en septembre 2014 qui tient dans un document[10] pdf de 30 pages. Ces chiffres ne couvrent que les ACs reconnues par Mozilla et/ou Microsoft.

C'est ce que l'on appelle le problème d'interopérabilité. Peter Smith a mis en exergue la complexité de ce problème ainsi : « [PKI] interoperability is something of a will-o'-the-wisp. You think you understand what people mean by it, and then quickly realize that you don't. In my experience, it's possible when discussing interoperability to be at cross-purposes for all of the time. Interoperability between members of the same PKI is axiomatic. Certificates issued by one bank should be recognizable by another. Interoperability becomes an issue when it is between different PKIs » (Smith 2000). Si un groupe d'experts a du mal à solutionner ce problème, comment imaginer qu'un particulier sans compétence particulière le puisse ?

Plusieurs méthodes ont été proposées pour gérer la confiance dans les ACs. Nous pouvons les regrouper en deux approches. La première est ad-hoc et consiste en des listes d'ACs de confiance dans les applications et maintenues par les vendeurs de logiciels ; par exemple comme pour les navigateurs web. Cette solution est imparfaite pour les diverses raisons expliquées précédemment. De plus, quelle relation de confiance existe-il entre un vendeur de logiciel et ses utilisateurs ? Cette question est pertinente lorsque l'on voit des pratiques comme celle de Lenovo qui met en œuvre des attaques de

[9] http://mxr.mozilla.org/mozilla-central/source/security/nss/lib/ckfw/builtins/certdata.txt?raw=1

[10] http://social.technet.microsoft.com/wiki/contents/articles/14215.windows-and-windows-phone-8-ssl-root-certificate-program-member-cas.aspx

falsification de certificats pour injecter de la publicité[11]. La deuxième approche consiste à créer des relations de confiance entre ICPs directement avec des méthodes de certification croisée. Cependant, cette approche de relation entre CAs ne fonctionne que dans un contexte fermé puisqu'aujourd'hui le monde des ICPs consiste à un ensemble d'îlots isolés.

Notre travail de recherche s'est donc porté sur deux questions :

1. Comment créer de la confiance dans un monde ouvert formé d'ICP isolées ?
2. Comment permettre à un utilisateur lambda sans compétence particulière d'être assez informé pour prendre une décision de confiance éclairée ?

Pour répondre à ces deux questions, nous avons tout d'abord proposé de changer le modèle de confiance à trois entités du standard X.509 en ajoutant une quatrième entité, appelée mandataire de confiance, qui évalue les ACs pour les EDs. Ce nouveau modèle a été proposé à l'IUT-T qui après vote l'a ajouté dans le futur standard X.509 qui devrait paraître en 2016. Le mandataire de confiance fournit à ses EDs le niveau d'assurance des certificats des ACs ainsi que toute information complémentaire telle que le niveau de garantie sur les transactions offert par l'AC.

5.2 Le problème de l'interopérabilité entre ICPs

Alors que cette technologie est disponible depuis une quinzaine d'années, les certificats électroniques restent peu déployés au regard des bénéfices en terme de protection qu'ils apportent par rapport au classique login/mot de passe. En 2003, le comité technique de l'OASIS a mené une enquête sur les raisons qui empêchent l'adoption générale de cette technologie (Hanna et al. 2004). Parmi les résultats obtenus, nous pouvons retenir les obstacles suivants :

1) Problèmes d'interopérabilité entre ICP
2) Trop de travail légal nécessaire
3) Difficile d'utilisation pour les utilisateurs finaux
4) ICPs sont peu comprises

Le déploiement des ICPs dans le modèle ouvert nécessite des régulations aux niveaux juridiques, organisationnels et techniques. Des différences culturelles et économiques ainsi que des approches différentes sur le rôle que les gouvernements doivent jouer à l'intérieur des frontières géographiques, contribuent à la mise en place de cadres juridiques et techniques différents entre les pays. Ils sont à la source des problèmes d'interopérabilité constatés dans les ICPs. Nous avons exprimé ce problème par un modèle en trois couches (Figure 37). Je présente par la suite un résumé de (Wazan et al. 2013) afin de montrer la difficulté à harmoniser ces trois niveaux.

[11] http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

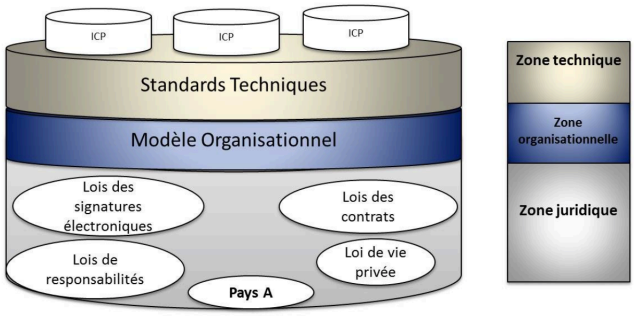


Figure 37. Les niveaux de régulation des ICPs

5.2.1 Différences juridiques

La mise en place des ICPs nécessite le traitement de questions juridiques à différents niveaux. Nous soulignons dans cette section la différence entre les juridictions quant à la façon de reconnaitre les signatures électroniques, la validité des contrats électroniques, et les responsabilités juridiques des ACs, des PdCs, et des EDs les uns vis-à-vis des autres. Enfin nous montrons les différentes approches qui ont été suivies en ce qui concerne la régulation juridique de la vie privée. Généralement, ces différences juridiques existant aujourd'hui proviennent de traditions juridiques différentes. Il existe deux traditions différentes : la tradition common-law dont le principe est de s'appuyer sur le précèdent judiciaire pour apprécier les affaires juridiques, et la tradition civil-law qui s'appuie sur l'existence de lois plutôt que des règles des tribunaux pour apprécier les affaires juridiques (American Bar Association 2001).

5.2.1.1 Différences légales pour la reconnaissance des signatures électroniques

Il existe trois approches essentielles pour traiter les technologies de signatures électroniques peuvent être identifiés: (a) l'approche indépendante de la technologie; (b) l'approche dépendante de la technologie, et (c) l'approche hybride (UNCITRAL 2009).

L'approche indépendante de la technologie est basée sur le principe de neutralité technologique qui accorde un effet légal minimum à toutes les technologies. Le principe de neutralité technologique permet de s'assurer que la législation reste valable même lorsque les technologies deviennent obsolètes. Cette approche est souvent suivie dans les pays de tradition common-low tels que les États-Unis, le Royaume-Uni, et l'Australie. Selon cette approche, les signatures électroniques sont équivalentes aux signatures manuelles si elles remplissent certaines fonctions. En cas de litige, la validité de la signature électronique est établie a posteriori par un juge, ou par une autorité publique (UNCITRAL 2009).

Dans *l'approche dépendante de la technologie*, la loi favorise une seule forme de signature électronique (d'habitude les signatures numériques). Pour cela, les lois précisent des exigences techniques et financières imposées aux ICPs pour qu'une signature électronique soit validée.

L'inconvénient de cette approche est qu'elle rend incertaine le statut juridique des autres types de signatures électroniques. D'un autre côté, cette approche permet aux parties impliquées dans une communication établie dans une juridiction donnée d'être certaines de la validité des signatures exploitées.

L'*approche hypbride* combine les caractéristiques des deux approches précédentes. Cette approche est souvent suivie dans les pays de tradition civil-law. Elle assure un équilibre entre la flexibilité et la certitude en fixant des exigences minimales pour tous les types de signatures électroniques et en même temps elle attribue un effet juridique clair pour certaines formes des signatures électroniques qui sont conformes à des exigences techniques spécifiques. Au niveau minimum, la signature électronique ne peut être juridiquement refusée au seul motif qu'elle est sous forme électronique. L'Union Européenne, qui est formée de pays ayant des traditions juridiques différentes, a adopté cette approche à travers la directive 1999/93/EC sur les signatures électroniques.

5.2.1.2 Différences légales pour la validité d'un contrat électronique

Il existe deux types de contrats électroniques : le contrat au clic « clickwrap contract » et le contrat à la navigation « browsewrap contract » (Moringiello et al. 2008). Le contrat au clic est un contrat auquel un consommateur doit donner son accord en cliquant sur l'icone « J'accepte » avant de compléter la transaction. Les contrats à la navigation, qui sont souvent accessibles avec des liens étiquetés «politiques d'utilisation» ou «conditions d'utilisations», sont appelées ainsi car au sein de ces contrats, un utilisateur du site web se soumet aux obligations contractuelles en en navigant tout simplement le site web. En d'autres termes, les contrats browsewrap caractérisent tout contrat ne nécessitant pas une manifestation explicite du consentement.

Les contrats électroniques, qu'ils soient de type clickwrap ou browsewrap, sont des contrats d'adhésion. Ces contrats ne permettent pas la négociation entre les partenaires ; on les accepte tels quels ou on les refuse. Ils sont souvent conclus entre des partenaires de négociation qui se trouvent dans des positions inégales, comme lorsqu'un client individuel se voit attribuer un contrat par un vendeur. Ces contrats soulèvent en général des questions quant à l'équité et au consentement (voire de l'abus de positon dominante).

Certains pays comme les Etats-Unis tendent à régulariser les contrats électroniques principalement en se basant seulement sur les lois traditionnelles des contrats, tandis que d'autres pays, comme l'Europe, ajoutent aux lois traditionnelles des extensions différentes (Deffains et al. 2008).

Les lois réglementant les contrats de consommation en général et les contrats d'Internet, en particulier, divergent entre les États-Unis et l'UE en grande partie à cause de la directive européenne sur les clauses abusives des contrats (qui réglemente les contrats sous forme offerts par les commerçants aux consommateurs que ce soit en ligne ou hors ligne), la directive européenne sur la vente à distance (qui réglemente les transactions entre les commerçants et les consommateurs à

distance soit par le biais de la télévision, le télémarketing, l'Internet ou tout autre moyen de communications électroniques) (Deffains et al. 2008). L'annexe 1 de la directive de l'UE sur les clauses abusives des contrats contient une liste des termes qui peuvent être considérés comme abusifs. En France, la directive a été étendue par la législation nationale en ajoutant que l'utilisation de la langue française est obligatoire. Bien que des pays comme le Canada, l'Australie et la Grande Bretagne partagent la même culture juridique que les Etats Unis, leurs approches de protection des consommateurs ressemblent plus à l'approche européenne (Bix et al. 2006).

Dans le cadre des ICPs, le consommateur peut être à la fois le PdC et l'ED. En raison de la nature lointaine de l'ICP, aujourd'hui les ICPs tendent à régulariser leurs relations avec les PdCs et les EDs à travers des contrats électroniques plutôt que des contrats écrits. Ces contrats contiennent généralement des informations sur : la responsabilité et les obligations des PdCs (resp. des EDs) vis-à-vis les ICPs et les EDs (resp. les PdCs), la responsabilité des ICPs vis-à-vis les PdCs (resp. les EDs), l'identification de la juridiction où le litige sera examiné en cas de problèmes, l'identification de la juridiction qui pourra pour régler un différent, les procédures d'arbitrage avant le dépôt des plaintes contre les ICPs, la limitation de responsabilité des ICPs, et les règles liées au traitement des informations personnelles (pour les PdCs).

Les contrats entre les ICPs et les PdCs sont généralement de type « clickwrap », car les ICPs demandent toujours le consentement des PdCs au moment où les certificats leur sont délivrés. Les contrats électroniques pour les EDs sont de type « browsewrap » car les liens des contrats sont positionnés dans les extensions des certificats. Un utilisateur jouant le rôle d'une ED doit afficher le certificat et ensuite il doit inspecter les extensions de certificats pour trouver le lien vers son contrat électronique. Etant donnée la difficulté d'accès à ce contrat, il nous semble difficile qu'il soit validé par les tribunaux, compte tenu que les EDs n'ont même pas conscience de l'existence de certificat ni de son utilité. En Europe, si le consommateur n'a pas donné son accord de manière explicite avant la conclusion de la transaction le contrat n'est pas valide (point d de la directive). De même aux Etats Unis, ce contrat peut être considéré comme insuffisant par les tribunaux si les ICPs ne peuvent pas prouver que les EDs ont pris connaissance des conditions des certificats préalablement à l'utilisation. Enfin, la validité de certaines clauses des contrats de PdCs n'est pas certaines dans certains pays, en particulier les clauses concernant le lieu de résolution de litige.

5.2.1.3 Différences sur la responsabilité des parties impliquées

Les questions de responsabilité jouent aussi un rôle important dans la relation entre les entités dépendantes (EDs), les porteurs des certificats (PdCs) et les ICPs, mais aussi entre les ICPs elles-mêmes. Les EDs et les PdCs peuvent se demander quand et dans quelle mesure ils seront indemnisés si une ICP n'a pas réussi à délivrer un certificat ou si elle a échoué en révoquant un certificat.

Plusieurs pays ont tenté de régulariser explicitement la relation entre les ICPs, les PdCs et les EDs, tandis que d'autres restent complétement silencieux. Les approches législatives qui ont été adoptées pour le traitement de la responsabilité des parties peuvent être catégorisées comme suit:

- Pas de dispositions spécifiques sur les standards de conduite ou sur la responsabilité comme aux Etats-Unis,
- Des standards de conduite et des règles de responsabilité seulement pour les fournisseurs des ICPs comme dans l'UE,
- Normes de règles de conduite et de responsabilité pour les PdCs et les fournisseurs des ICPs comme en Chine,
- Normes de conduite et des règles de responsabilité pour toutes les parties comme cele a été proposé par les nations unies.

Les différences entre juridictions apparaissent également sur la désignation de l'entité qui a la charge de porter la preuve ; en cas de problème, qui doit prouver le problème l'ED/PdC ou l'ICP ? Il y a globalement deux positions à ce niveau : négligence ordinaire (il revient à la partie lésée de démontrer que le dommage a été causé par la violation des obligations de l'autre partie), négligence présumée (la faute d'une partie est présumée lorsque le dommage résulte d'un acte qui lui est attribuable), et la responsabilité stricte.

Les fournisseurs de services de certification recherchent donc systématiquement et autant que possible à limiter leurs responsabilités envers les PdCs et les EDs. Sur cet aspect aussi, il existe des différences. Bien que la plupart des systèmes juridiques reconnaissent généralement le droit des parties participant à des contrats à limiter ou exclure leurs responsabilités grâce à des dispositions contractuelles, ce droit est généralement soumis à diverses restrictions et conditions (UNCITRAL 2009).

5.2.1.4 Règles liées au respect de la vie privée

Les ICPs ont besoin de collecter un ensemble de données personnelles et d'informations commerciales sur les personnes qui demandent des certificats. Ces informations doivent être conservées par les ICPs pour des utilisations futures. Les ICPs doivent donc prendre les mesures nécessaires pour assurer que l'accès à ces informations soit conforme aux lois applicables sur la protection de la vie privée. Les gouvernements ont adopté différentes approches pour régulariser les règles juridiques liées à la vie privée. La différence entre l'approche européenne et américaine quant à la régulation sociale et économique ne peut être plus claire dans le domaine de la protection des informations personnelles. En Europe, la protection des informations privées est considérée comme un droit humain fondamental. Aux États-Unis en revanche, celui qui collecte et stocke des informations privées est censé en être le propriétaire, à moins qu'une loi spécifique ne crée une telle obligation pour

un type précis des informations personnelles, n'est normalement pas responsable pour les utilisations des données collectées (Winn 2009).

5.2.2 Les différences organisationnelles

La façon dont les ICPs sont structurées varie d'un pays à un autre selon le niveau d'intervention du gouvernement concerné. L'intervention des gouvernements est considérée dans la plupart des pays comme un moyen de renforcement de confiance. De plus, le niveau de maturité technologique et administrative d'un pays joue un rôle très important dans la détermination du modèle organisationnel approprié pour les ICPs. Trois modèles principaux peuvent être identifiés (UNCITRAL 2009):

- Autorégulation : Selon ce modèle, le domaine d'authentification est laissé ouvert. Alors que le gouvernement peut créer un ou plusieurs schémas d'authentification au sein de ses propres services, le secteur privé est libre de mettre en place des schémas d'authentification, commerciale ou autre, comme il l'entend. Il n'existe pas d'autorité d'authentification de haut niveau et les fournisseurs de service d'authentification sont eux-mêmes chargés d'assurer l'interopérabilité avec d'autres fournisseurs, nationaux ou internationaux, selon les objectifs de l'établissement du schéma d'authentification. Aucune approbation de licence pour les prestataires de services d'authentification n'est nécessaire. Les Etats-Unis sont l'exemple le plus connu pour la mise en œuvre de ce modèle.
- Intervention limitée des gouvernements : certains gouvernements établissent un système d'accréditation volontaire de telle sorte que les prestataires des services ICPs n'aient pas besoin de posséder une licence. Ceux autorisés bénéficient d'avantages par rapport aux prestataires non-certifiés. L'inspection (l'audit) des ICPs se fait normalement par des entités accréditées par le gouvernement concerné. Singapour et l'Europe sont des exemples de ce modèle.
- Intervention complète des gouvernements : Les gouvernements mènent une procédure d'accréditation obligatoire envers les prestataires de services ICP. Ils mènent également le processus d'audit. Dans certaines situations l'intervention de l'état va jusqu'au monopole d'état pour la mise en place des ICPs. La Chine et la Malaisie suivent ce modèle.

5.2.3 Différences techniques

Garantir l'interopérabilité technique entre des solutions technologiques, des procédures, des systèmes et des applications, tant aux niveaux nationaux que aux niveaux internationaux, est principalement liée à l'adoption des standards.

Les standards ICT (Information & Communication Technology) vont de standards *de facto* issus de la popularité d'une technologie propriétaire, à l'adoption de solutions promues par des

organismes privés informels appelés « consortiums » qui travaillent généralement hors du contrôle des régulateurs nationaux (Winn et al. 2008), sans oublier bien sûr les standards *de droit* produits par des organismes reconnus nationalement ou internationalement telles que l'Union Internationale des Télécommunications (ITU), l'ISO, etc. Les architectures propriétaires conduisant à des standards *adhoc* ne sont pas ouvertes, et le plus souvent des artifices mis en œuvre au sein de ces technologies peuvent amener à annihiler toute concurrence éventuelle et/ou souhaitable. En revanche, les standards ICT développés par l'IETF ou le W3C sont ouverts et distribués gratuitement sur Internet et, si possible, mis à disposition sur une base libre à l'écart de toute propriété intellectuelle qui pourrait être dans d'autres circonstances nécessaire pour mettre en œuvre ces standards (Winn 2006).

Aux États-Unis, la plupart des standards sont élaborés par des organisations privées de développement des standards, tels que l'Institute of Electrical and Electronics Engineers (IEEE) ou des consortiums comme CA/Browser Forum. Par la suite, ces standards sont proposés à l'American National Standards Institute (ANSI) pour qu'ils soient reconnus comme « American National Standards », puis à des organismes internationaux tels que l'ISO. Par exemple, plusieurs standards ad-hoc existent aux Etats-Unis dans le cadre des ICPs. En particulier, le standard « extended validation » (CA/Browser Forum 2014) décrit un ensemble de critères techniques et juridiques que les ICPs doivent respecter pour pouvoir générer ce type de certificat utilisé pour l'authentification des serveurs web. Le standard est mis en place par un regroupement d'ICPs commerciales avec les concepteurs et développeurs des navigateurs Web les plus connus comme FireFox, Internet Explorer, etc.

Dans les pays européens, le travail de l'élaboration des standards est souvent traité comme une partie de la mise en œuvre des politiques économiques nationales. En conséquence la surveillance des gouvernements sur le développement des standards est souvent considérée plus légitime en Europe qu'aux États-Unis. Ces organismes nationaux de standardisation (ONS), tels que le British Standards Institute, l'Association Française de Normalisation, ou le Deutsches Institut für Normung, sont des organisations non gouvernementales, mais qui en pratique ont une relation étroite avec les entités gouvernementales chargées de la supervision et de la réglementation de l'économie de leurs gouvernements respectifs. L'Europe a adopté une stratégie appelée « la nouvelle approche » visant à harmoniser les efforts des réformes des lois avec les efforts de développement des standards entre les états membres. La directive européenne sur les signatures électroniques est une version allégée de la nouvelle approche, car la procédure pour déterminer les standards techniques qui seraient considérés conformes à la loi a été simplifiée. Dans ce cadre, l'ETSI a proposé par exemple les « qualified certificates » (ETSI 2007) qui s'est retrouvé en concurrence avec l' « extended validation certificate » du CA/Browser Forum.

Récemment, le CA/Browser Forum (CA/Browser Forum 2014) et l'ETSI (ETSI 2011) ont travaillé sur l'interopérabilité de leurs standards techniques respectifs. Seulement, cette harmonisation ne vaut qu'entre les Etats-Unis et l'Europe et pour un type de certificat dédié aux serveurs web. De nouveaux pays commencent à avoir un rôle important dans les développements des standards au

niveau mondial (en particulier la Chine, l'Inde et la Corée). Scott Kennedy (Kennedy 2006) décrit l'investissement de la Chine dans la guerre de développement des standards pour briser la domination de l'occident sur ce domaine. Il y aura donc peut-être de nouvelles parties prenantes à considérer.

Nous pouvons donc synthétiser le problème d'interopérabilité avec la Figure 38 (pour rappel la liste de confiance de Mozilla contient 82 ACs de 89 ICPs provenant de 30 pays). Or, selon le modèle X.509, les EDs sont censées extraire les facteurs de confiance techniques et juridiques des documents PC/DPC, afin de pouvoir décider si un certificat est suffisamment digne de confiance ou pas. Le standard X.509 déclare que « The certificate user may be bound to its obligations under the certificate policy by the act of importing an authority public key and using it as a trust anchor, or by relying on a certificate that includes the associated policy identifier. ». Dans le même sens, le standard ad-hoc RFC 5280 (Housley et al. 2008), qui définit le profil X.509 pour l'Internet, est plus clair et déclare que : « A certificate user should review the certificate policy generated by the certification authority (CA) before relying on the authentication or non-repudiation services associated with the public key in a particular certificate ». Ceci est bien évidemment impossible. Différentes techniques ont donc été construites pour aider l'ED dans cette tâche.

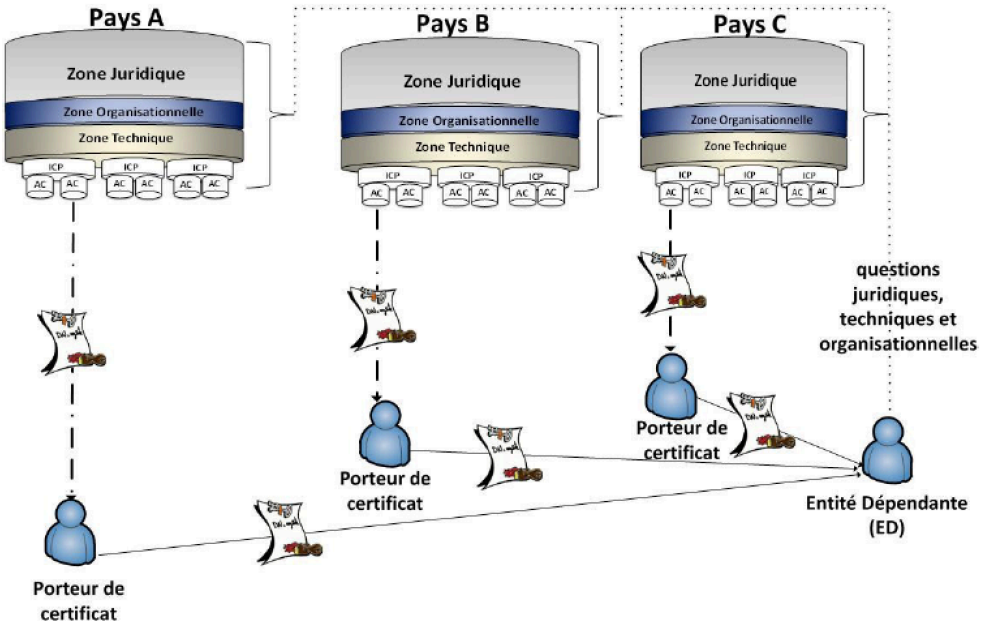


Figure 38. Problème d'interopérabilité

5.3 Techniques actuelles d'interconnexion d'ICPs

Il existe plusieurs approches permettant à une ED d'avoir confiance dans un certificat. Ces approches comprennent deux mécanismes :

- Un processus contractuel pour reconnaître les ACs. Ce processus a pour objectif de démontrer qu'une AC répond aux exigences légales et techniques à la fois en terme de crédibilité et d'interopérabilité ;

- Un mécanisme pour propager la reconnaissance des ACs de confiance sur l'ordinateur de l'ED. Il fournit des informations à propos de la confiance d'une AC dans un format reconnu par l'ordinateur afin que le logiciel de l'ED puisse automatiquement accepter ou refuser un certificat électronique. Cela est effectué par la pré-configuration d'une racine de confiance sur le système de l'ED. Ensuite, les chaînes de certification peuvent être échangées par un protocole applicatif. Si la chaîne démarre avec une autorité racine de confiance alors toutes les ACs de la chaîne sont considérées comme sûr. Dans le cas contraire, aucune des ACs n'est reconnue comme sûre.

Nous pouvons classifier ces approches en deux catégories : 1) la topologie de confiance est gérée par les ACs elles mêmes, ou 2) une liste de racines de confiance est gérée par les EDs ou des tiers de confiance.

5.3.1 Topologies de confiance inter-ACs

Les ACs peuvent créer des topologies de confiance au lieu laisser cette tâche à des EDs non expérimentées. L'idée générale est que chaque ED a confiance dans une AC qui certifie d'autres ACs pour ses EDs. Dans ce type de topologie, l'AC joue donc deux rôles : celui de gestionnaire de certificats et celui de recommandeur de certificats.

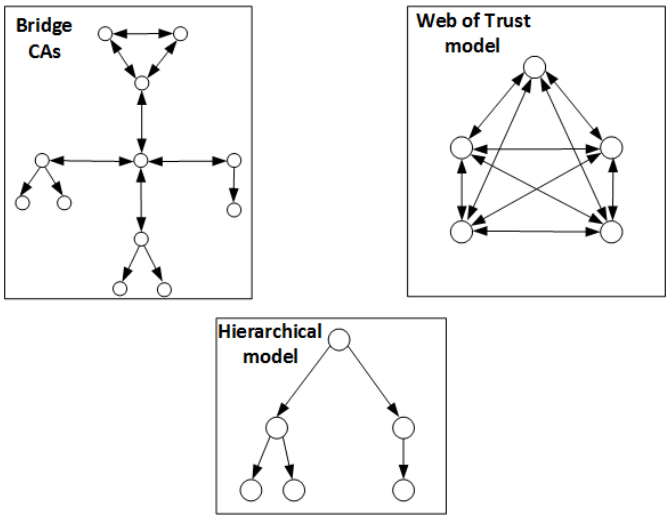


Figure 39. Topologies de chaînes de confiance

Les chaînes de confiance peuvent être organisées en hiérarchie, en toile ou au travers d'une passerelle. Chaque flèche de la Figure 39 définit le sens du lien de confiance. Dans la topologie hiérarchique, le flux de confiance part d'une AC supérieure vers des AC subordonnées. Dans la toile de confiance, la structure est plus anarchique. Enfin, l'utilisation d'une passerelle de confiance simplifie la gestion en centralisant en un point unique la gestion des interconnexions. Ces topologies créent des chemins de certification l'AC de l'ED et le certificat du PdC. Par conséquent, elles fournissent un mécanisme de transmission de la reconnaissance de certificats entre domaines de confiance interconnectés. Quelque soit la topologie, ces structures de confiance sont construites sur un

processus appelé certification croisée qui comprend une évaluation légal, politique et technique. Cependant, ce processus n'est pas standardisé et plusieurs propositions plus ou moins bien détaillées cohabitent telle que l'infrastructure à clé publique fédérale des Etats-Unis FPKI (FPKIPA 2012).

Les approches inter-ACs sont appropriées dans le contexte de déploiement fermé. Par contre, elles ne peuvent être utilisée dans le monde ouvert où toutes les ACs seraient interconnectées. A première vue, on pourrait imaginer une infrastructure composée d'ACs nationales qui certifieraient des ACs subordonnées qui dépendraient de leur juridiction. Seulement, ces topologies ne sont pas viables pour des raisons techniques de part la difficulté de gestion des longs chemins de certification (Polk et al. 2000). De plus, cette approche ressemblerait à un système d'accréditation général où chaque AC serait certifiée par son autorité nationale. Comme cela a été expliqué dans la section précédente, les différences organisationnelles entre pays ne le permettraient pas. De même, une certification croisée (via une passerelle ou non) entre tous les pays du monde sera extrêmement difficile à réaliser car nécessite une harmonisation légale générale. Enfin, quel processus de certification croisée choisir ? Il n'existe pas de norme internationale aujourd'hui.

5.3.2 Reconnaissance gérée par les EDs ou des tiers de confiance

La confiance dans un certificat peut être recommandée par toute entité indépendante des ACs. L'idée générale est que les utilisateurs dans une communauté d'intérêt particulière puisse obtenir des recommandations du leader de cette communauté sur les certificats impliqués dans leurs transactions électroniques. Ce recommandeur peut être un gouvernement (par exemple GateKeeper en Australie (AGIMO 2009)) ou une entreprise privée (comme Microsoft ou Mozilla).

En général, les recommandeurs créent une liste d'exigences minimales et reconnaissent les certificats des ACs qui correspondent à ce minimum requis (par exemple, pour Microsoft[12] ou Mozilla[13]). Souvent ces exigences minimales sont faibles et garantissent donc un niveau d'assurance faible.

Contrairement aux approches inter-ACs, il n'y a qu'un moyen de transmission de la confiance qui est la *liste de confiance*. Il n'y a pas d'homogénéisation sur les listes de confiance. Dans certains cas, il s'agit de simples fichiers (par exemple, les magasins de certificats des navigateurs web) que l'ED peut modifier à son gré. Dans d'autres cas, il s'agit de listes signées par le recommandeur que l'ED ne peut modifier. D'un point de vue interopérabilité, la liste de confiance remplace les certificats croisés. Et donc, le recommandeur jour le rôle de racine de confiance.

Lorsque l'utilisation de la liste de confiance est associée à un processus politique, on parle de processus de reconnaissance croisée. L'APEC le définit ainsi : « An interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to

[12] https://technet.microsoft.com/en-us/library/cc751157.aspx

[13] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/

authenticate a subject in the other PKI domain, and vice versa" (Asia PKI forum 2005). Aujourd'hui, le processus de reconnaissance croisée n'est pas normalisé. Par exemple, le processus de reconnaissance du GateKeeper australien (AGIMO 2009) fournit un processus d'accréditation pour les organisations et les fournisseurs de service voulant utiliser leurs certificats avec des agences gouvernementales. Le processus GateKeeper nécessite une harmonisation des politiques des domaines ICPs en prouvant qu'elles sont comparables avec celles de GateKeeper.

Cette approche de reconnaissance, étant indépendante des ACs et ne nécessitant pas de chemins de certification, est plus appropriée au monde ouvert. Cependant, plusieurs reproches peuvent être émis. Tout d'abord, la relation entre l'ED et son recommandeur n'est pas claire dans le cas des navigateurs Web. Dans le cas de GateKeeper, il s'agit d'un monde fermé limité aux agences gouvernementales. Le processus de reconnaissance croisée est manuel et non reproductible. Enfin, les recommandations fournies aux EDs sont binaires (reconnu ou non reconnu). Ceci ne permet pas à l'ED d'être éclairé dans sa décision de confiance.

5.4 Un nouveau modèle de confiance pour les ICPs

Pour répondre à ces différentes questions nous avons proposé une nouvelle approche unifiée (i.e., couvrant les besoins des mondes fermés et ouverts).

5.4.1 Un modèle à quatre entités plus juste pour l'entité dépendante

Dans le monde fermé, l'administrateur de l'ICP de chaque organisation joue le rôle d'un expert technique et juridique pour aider les employés de cette organisation dans le traitement de validation d'un certificat venant d'une autre organisation (Figure 40). Toutes les EDs sont ainsi aussi des PdCs provenant de l'AC de leur organisation. De plus, comme les EDs et l'expert font partie de la même organisation/entreprise, la relation de confiance entre les EDs et l'expert est créée naturellement. Cette confiance des EDs envers les administrateurs n'est pas seulement liée à la qualité des certificats qu'ils fournissent mais aussi à leurs capacités à recommander des ACs d'autres organisations avec lesquelles leur organisation à décider de collaborer. Les décisions des EDs sont ainsi automatisées car les topologies d'interconnexion sont souvent construites pour un nombre de services clairement défini à l'avance correspondant aux besoins de collaboration entre les organisations. Ceci permet aux administrateurs de prendre en considération toutes les précautions nécessaires.

Dans le monde ouvert, la situation est beaucoup plus complexe pour plusieurs raisons:

- Les ACs et les experts sont des entités différentes.
- Il n'existe pas forcément de relation prédéfinie entre les EDs et les experts. Les EDs ne font pas partie d'une communauté existante comprenant un expert technique et juridique.

- Les EDs et les PdCs sont des entités séparées. La plupart des EDs n'ont pas de certificats et ne connaissent même pas l'intérêt réel des certificats.
- Le nombre de services n'est pas prédéfini comme dans le modèle fermé. Les ACs ont tendance sous ce modèle de générer des certificats de type « *one size fits all* » pour un nombre non-défini de services.

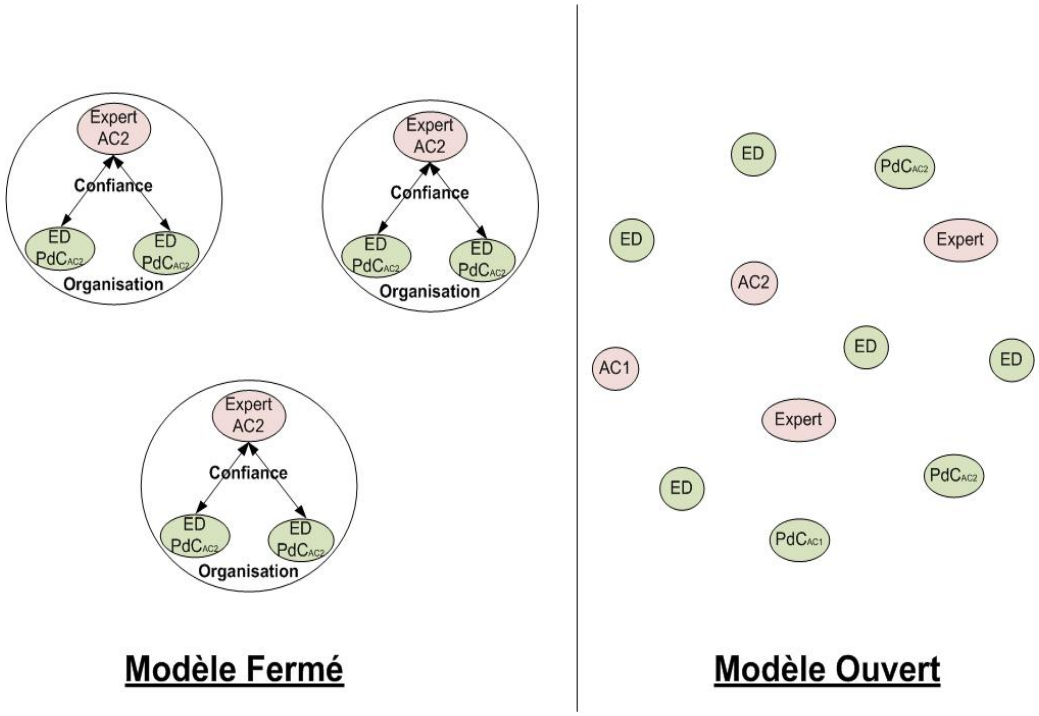


Figure 40. Différences entre modèle fermé et modèle ouvert

Dans le modèle ouvert, les EDs ont aussi besoin d'un expert technique et juridique pour les aider à prendre les décisions correctes sur les certificats. Les tierces parties, comme le navigateur web qui définit une liste de confiance, occupent implicitement ce rôle. A partir de ce constat, nous avons proposé une architecture unifiée pour les deux modèles de déploiement des ICPs. En effet, quel que soit le contexte de déploiement (fermé ou ouvert), les EDs ont les mêmes besoins dans leur prise de décision, i.e. un expert technique et juridique. Les différences se situent au niveau des entités qui jouent ce rôle d'expert, de la relation de confiance prédéfinie ou non entre cet expert et les EDs et de l'information que cet expert propose aux EDs. Nous avons donc défini de manière explicite cette entité dans le modèle de confiance de X.509 et nous l'avons appelée mandataire de confiance (TB pour Trust Broker), (Figure 41). Nous avons proposé ce modèle au groupe 17 de l'ITU-T via David Chadwick qui est représentant UK. Notre proposition, après vote, a été retenue et est donc partie intégrante du document de travail de la version 8 de la norme ISO/IEC 9594-8 / ITU-T X.509[14] qui devrait apparaître en 2016.

[14] http://www.x500standard.com/index.php?n=Ig.X509ext

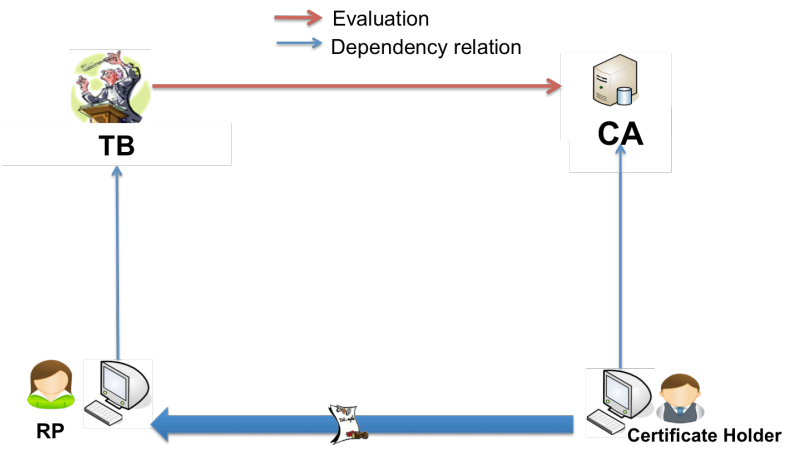


Figure 41. Le nouveau modèle de confiance X.509 à quatre entités

Notre idée principale est de séparer explicitement le rôle de gestionnaire de certificat de celui d'expert technique et juridique pouvant donner des recommandations. Ainsi dans ce nouveau modèle, chaque entité a une tâche/responsabilité bien précise :

- Les ACs sont responsables de la gestion du cycle de vie des certificats,
- Les PdCs sont responsables de la bonne utilisation de leurs certificats,
- Les EDs sont responsables de la prise de décision d'accepter ou non un certificat,
- Les mandataires de confiances sont responsables de l'évaluation des ACs (Analyse des documents CP/CPS, rapports d'audit, etc.)

L'objectif du mandataire de confiance est d'évaluer objectivement les ACs et d'envoyer des recommandations aux EDs pour les aider à prendre des décisions éclairées sur les certificats. Pour cela, il doit être indépendant des ACs. Ainsi, le modèle de confiance est plus juste vis à vis des EDs car maintenant ils ont un expert technique et juridique qui les aide. Dans notre modèle, l'ED ne dépend plus directement des ACs mais uniquement des recommandations du mandataire de confiance. Le mandataire de confiance doit traiter directement chaque AC indépendamment de toute structure de confiance dans laquelle l'AC pourrait se trouver. Ainsi, les chemins de certification/validation des topologies inter-ACs n'ont plus de raison d'exister.

La relation entre le mandataire de confiance et les EDs doit être régularisée au travers d'accords contractuels dans lesquels le mandataire de confiance 1) reconnaît sa responsabilité envers les EDs sur ses recommandations et 2) s'engage à respecter la vie privée des EDs. Les accords entre EDs et mandataires de confiance créent des communautés de confiance. D'un autre côté, l'expert doit être indépendant des ACs, sa relation avec les ACs doit également être régulée par des accords explicites, de sorte que l'expert puisse transférer la responsabilité à une AC lorsqu'une fausse recommandation résulte d'une information erronée fournie par une AC. Plusieurs stratégies de mise en oeuvre peuvent être envisagées : 1) des services commerciaux dont le métier consiste à fournir des recommandations sur des certificats, ou encore 2) les nations peuvent jouer ce rôle pour leurs citoyens. Ainsi, notre

approche ne nécessite pas de normaliser les couches d'interopérabilité juridiques, organisationnelles ou techniques.

5.4.2 Le niveau d'assurance d'un certificat

Le mandataire de confiance doit fournir des informations qualitatives et quantitatives dans sa recommandation aux EDs. Le processus d'acquisition doit être dynamique (Figure 42). Lorsqu'un ED reçoit un certificat, il demande le niveau d'assurance de ce certificat au mandataire de confiance. Pour cela, il lui envoie les informations de l'AC ayant produit le certificat. Nous avons choisi cette méthode plutôt que d'envoyer le certificat directement pour des questions de protection de la vie privée. Ainsi le serveur mandataire n'a pas d'information sur les transactions de l'ED. En retour, le mandataire de confiance transmet à l'ED le niveau d'assurance du certificat (CLoA) ainsi que le niveau de confiance (CL) qui correspond au niveau de fiabilité de la valeur de CLoA retournée. Ajouté à cela, le mandataire de confiance donne des informations liées à l'utilisation du certificat (comme le niveau de protection financière). Aucun filtrage sur les informations fournies à l'ED n'est effectué par le mandataire de confiance. Ce traitement est réalisé par un détecteur de contexte qui se trouve au niveau de l'ED.

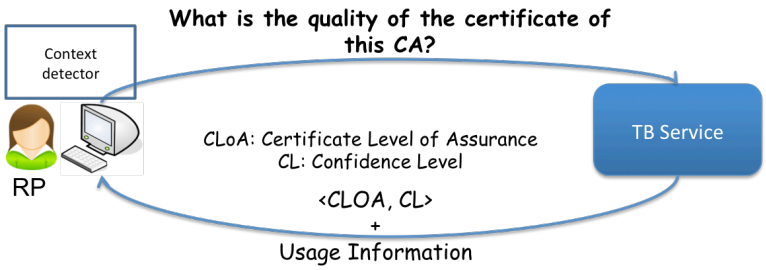


Figure 42. Processus d'acquisition des recommandations

Nous avons développé un module d'extension pour le navigateur web FireFox afin de montrer la faisabilité. Ce module modifie le traitement classique de validation des certificats suivi par FireFox pour suivre notre approche. La Figure 43 montre un exemple d'affichage de recommandation dans le cadre d'une transaction financière détectée par le module FireFox.

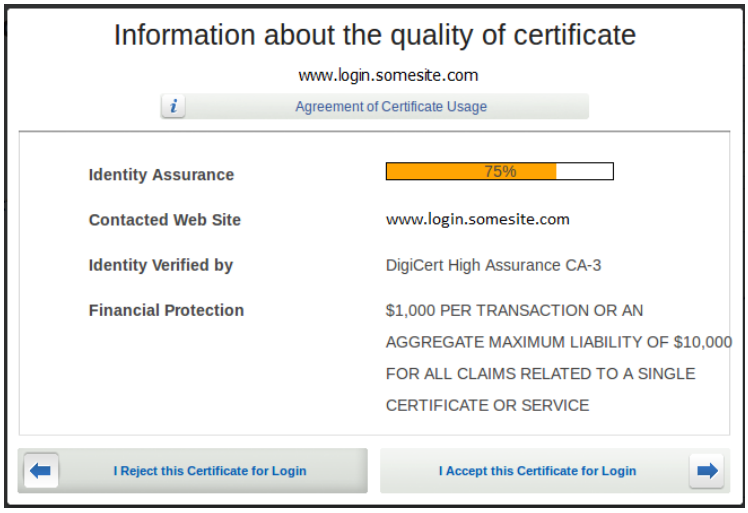


Figure 43. Exemple d'écran affiché à l'utilisateur

Le calcul du niveau d'assurance d'un certificat s'effectue par rapport aux trois documents représentant les pratiques de l'AC : La politique de certification (CP pour Certificate Policy), la déclaration des pratiques de certification (CPS pour Certification Practice Statement) et le rapport d'audit qui évalue la véracité des déclarations énoncées. Nous avons aussi montré que les EDs et aussi des mandataires de confiance voulant collaborer pouvaient fournir des compléments d'information sur l'analyse des certificats. Nous avons donc intégré toutes ces sources dans notre calcul :

$$\text{CLoA} = \sqrt[n]{CL * QoCA} * \text{QoCPS}$$

Où:

- QoCPS ∈ [0,1] représente la robustesse des procédures annoncées par l'AC dans les documents CP/CPS.
- QoCA ∈ [0,1] représente le niveau d'engagement de l'AC dans les procédures annoncées. Cette valeur est basée sur des recommandations de tierces parties qui surveillent les pratiques réelle de l'AC telles que les agences d'audit, ou les EDs elles mêmes.
- CL ∈ [0,1] est le degré de confiance que le mandataire de confiance a dans le calcul de la valeur de QoCA. Si le mandataire de confiance n'a que peu d'évidence sur l'engagement de l'AC, la valeur de CL sera faible.
- *n* est un entier pour contrôler l'impact que CL*QoCA sur le score final CLoA.

Les documents CP/CPS et rapport d'audit sont exprimés aujourd'hui en langage naturel. Il est donc difficile pour un expert d'évaluer manuellement chaque autorité de certification. Pour cela, nous avons proposé un processus semi-automatique qui permet à l'expert d'évaluer objectivement les ACs (Figure 44). Plus d'informations sur le calcul de QoCPS et QoCA ont été présentées dans (Wazan et al. 2011).

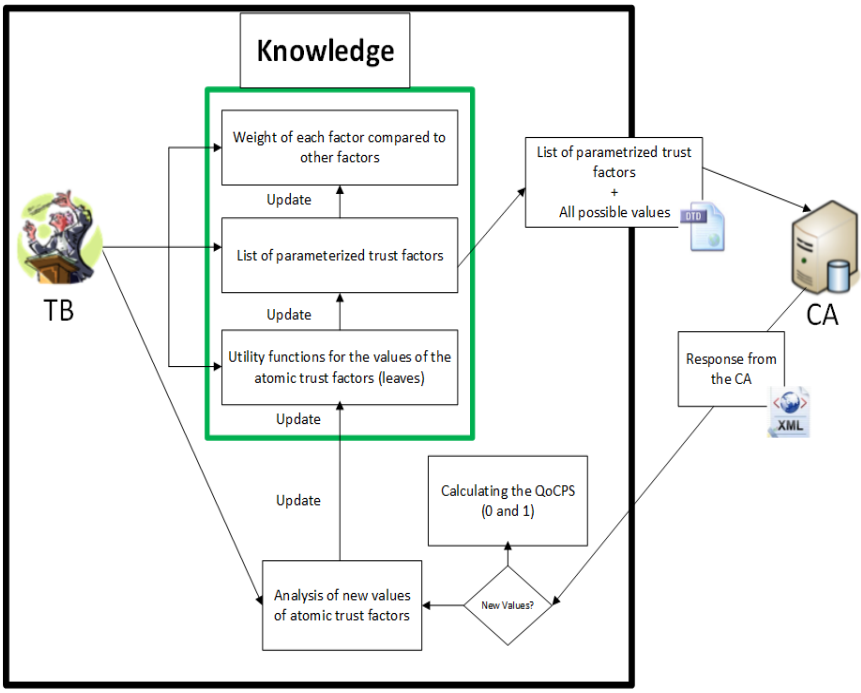


Figure 44. Processus semi-automatique d'évaluation

5.5 Bilan

J'ai présenté dans ce chapitre mes activités liées à la gestion de la confiance dans les infrastructures à clés publiques. Nous avons lancé cet axe de travail avec deux objectifs : informer l'utilisateur sur les certificats et préserver sa vie privée. Ainsi, nous complétons notre boucle de gestion en étudiant les étapes de récolte, calcul et affichage d'indicateurs de gestion de la sécurité (Figure 45).

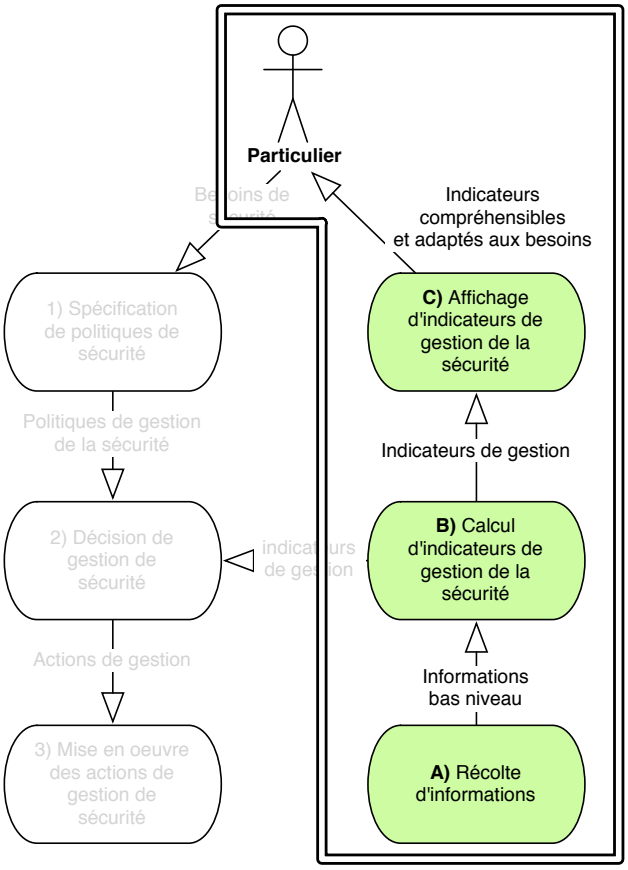


Figure 45. Eléments de la boucle de gestion traités dans le chapitre 5

Ce travail a fait l'objet de propositions de modifications du standard ITU-T X.509. Tout d'abord, l'étude menée sur la validation de certificats par les navigateurs web (Wazan et al. 2009) a montré des ambiguïtés dans le standard quant à la validation des extensions. Nous avons présenté une proposition de clarification sous la forme d'un « defect report » qui a été inclue dans le standard. Nous avons aussi proposé en avril 2013 notre modèle de confiance à quatre entités à au groupe d'étude 17 de l'IUT-T qui, après vote, a été accepté pour ajout dans la future version du standard. A la demande du groupe de travail de l'IUT-T, nous travaillons à la formalisation du protocole entre l'entité dépendante et le mandataire de confiance.

Je désire réellement continuer à travailler sur cet axe. En effet, il est anormal que l'utilisation des certificats électroniques ne soit pas plus répandue. Le couple identifiant/mot de passe est un mécanisme faible et pourtant il est toujours le plus utilisé. Il est assez anormal aussi que la grande majorité des messages échangés par courriel par exemple ne soit pas protégé. Il est donc nécessaire de proposer des moyens facilitant l'adoption et l'utilisation des certificats électroniques.

De plus, le problème d'hétérogénéité des processus de validation des certificats va être amplifié dans le futur avec les équipements mobiles (smartphones et tablettes) qui contiennent beaucoup de petites applications. Récemment, nous nous sommes rendu compte que beaucoup d'applications trouvées sur les magasins en ligne des systèmes d'exploitation pour équipements mobiles (Google Play store, Apple Store) ont leur propre gestion de la validation des certificats qui dans certains cas est

proche du néant total. Notre idée de mandataire de confiance peut simplifier cela en proposant un point unique choisi par l'utilisateur. De plus, il pourrait être envisageable d'externaliser le processus complet de validation en ajoutant ce nouveau service au mandataire de confiance. Toutefois, cela aura des implications sur la vie privée des personnes qu'il faudra résoudre.

Contrairement à mes travaux présentés précédemment qui portent sur la définition et la mise en œuvre d'une politique de sécurité dans le cadre d'une entreprise, travailler sur la protection des personnes m'a amené à considérer la problématique de la protection de la vie privée dans le cadre de mes recherches. Le chapitre suivant présente nos travaux de recherche sur cet aspect.

Chapitre 6. Aide à l'écriture de politiques d'autorisation pour la protection de la vie privée

Ces travaux ont été traité dans le cadre de la thèse d'Arnaud Oglaza (Oglaza 2014).

6.1 Présentation de la problématique

Aujourd'hui l'informatique personnelle qui consistait à un unique ordinateur personnel relié au réseau Internet via une connexion filaire par foyer tend à disparaître. Une étude réalisée par GFK/Médiamétrie publiée en nombre 2013[15] a montré que le nombre de foyers "multi-équipés" (ordinateur portable + téléphone mobile + tablette) a plus que doublé en un an et atteint les 4,7 millions de ménages en France. Ajouté à cela, les smartphones et tablettes ont aujourd'hui des capacités de traitement et de stockage permettant d'exécuter de nombreuses applications. A titre d'exemple, les français ont en moyenne 32 applications installées sur leurs smartphones Android selon le recensement effectué par Google en 2013[16] . Ce chiffre monte jusqu'à 40 applications dans des pays comme la Corée ou la Suisse. De plus, cette diversité d'équipements connectés à des réseaux informatiques va continuer à croître avec l'arrivée de l'Internet des Objets. Différentes études estiment que le monde compte déjà entre 15 et 20 milliards de "choses" connectées à l'Internet et que ce nombre devrait atteindre entre 50 et 80 milliards en 2020[17,18]. Toutes ces choses connectées et toutes ces applications peuvent être amenées à traiter et communiquer des données relatives aux personnes. Par conséquent, chaque personne va devoir contrôler toutes « ces choses et applications » si elle désire protéger sa vie privée.

Définir ce qu'est la vie privée et donc la protection de cette vie privée n'est pas chose simple. Si à la fin du 19ème siècle la vie privée était définie comme étant le droit de s'isoler (Warren et al. 1890), force est de constater qu'il est aujourd'hui difficile de s'isoler dans un monde numérique qui a été créé

[15] http://www.gfk.com/fr/news-and-events/press-room/press-releases/pages/gfkmédiamétrie-référence-des-equipements-multimédias-3ème-trimestre-2013.aspx

[16] http://think.withgoogle.com/mobileplanet/fr/

[17] http://www.zdnet.fr/actualites/80-milliards-d-objets-connectes-en-2020-39793776.htm

[18] http://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm

pour faciliter la circulation de l'information (Langheinrich 2009). Dans un récent article un peu polémique publié dans Rue 89 (Cauvin 2015), le blogueur E. Cauvin se demande même si la notion de vie privée peut exister dans notre monde numérique en faisant l'analogie entre notre mode de fonctionnement virtuel et l'émission de téléréalité « secret story » : « Notre vie connectée peut être de deux sortes : partagée, ou exposée » [sic]. De manière plus nuancée, les chercheurs vont aussi dans ce sens car on ne parle plus de s'isoler mais de tenter de contrôler ses informations personnelles dans le cadre d'activités liées à la collecte d'information, l'analyse d'information, la dissémination d'information ou l'invasion/interférence décisionnelle (Solove 2006). Ainsi, plusieurs définitions et formes de vie privée sont étudiées (Marx 2001; Solove 2006).

Pour répondre à cette problématique de contrôle de l'information, des chercheurs ont commencé à travailler sur la notion de technologies pour l'amélioration de la vie privée (en anglais Privacy-Enhancing Technologies ou PET) au début des années 80 (Chaum 1981; Pfitzmann et al. 1986). A cette époque, les solutions proposées portaient uniquement sur l'application de méthodes de chiffrement. Aujourd'hui, la recherche sur les PETs couvre un cadre beaucoup plus large et diversifié. Pour clarifier la profusion de solutions, je reprends ici la classification de (Danezis et al. 2010) qui au travers de trois propriétés montre les différentes facette de la protection de la vie privée. Tout d'abord, on peut voir la protection de la vie privée comme *un problème de confidentialité*. On y retrouve les solutions d'anonymisation des données (comme la k-anonymisation (Sweeney 2002) ou la l-diversité (Machanavajjhala et al. 2007)), les solutions d'anonymisation des communications (comme TOR (Dingledine et al. 2004) ou Blind (Ylitalo et al. 2006)) ou encore la minimisation des données collectées (comme le chiffrement homomorphe (Gentry 2009)). La protection de la vie privée peut aussi être envisagée comme *un problème de contrôle* où sont regroupés tous les travaux liés à la spécification et la mise en œuvre de politique d'autorisation. Cette catégorie regroupe les modèles de contrôle d'accès qui intègre des éléments propres à la vie privées, e.g. (Covington et al. 2006; Byun et al. 2005; Ajam et al. 2010; Byun et al. 2005), les langages/architecture pour exprimer et mettre en œuvre des politiques de protection de la vie privée, e.g. (Karjoth et al. 2003; Ardagna et al. 2009; Neisse et al. 2011) mais aussi les mécanismes de gestion d'identités comme décrits dans le chapitre 2. Enfin, une dernière façon d'améliorer la protection de la vie privée consiste à améliorer la transparence des services afin que les utilisateurs comprennent quelles données sont divulguées et comment elles sont utilisées. Par exemple, (Castelluccia et al. 2011) présentent quatre caractéristiques pour la transparence : 1) fournir des informations sur la façon dont les données sont collectées, stockées et analysées, 2) fournir un récapitulatif des données divulguées (à qui et dans quelles conditions), fournir un accès en ligne aux données personnelles et aux informations acquises grâce à leur traitement, et fournir un moyen d'évaluation des traitements par rapport aux lois et accords sur le respect de la vie privée, et 4) fournir un moyen d'éviter d'établir un profil utilisateur et informer sur la constitution des profils utilisateurs.

De part mes travaux précédents sur la gestion de la sécurité, nous avons naturellement traité le problème de protection de la vie privée d'un point de vue contrôle. Cependant, il n'était plus question de permettre à un administrateur qualifié de contrôler son système. Il fallait prendre en compte que celui qui définit la politique d'autorisation n'a aucune compétence en sécurité. Il est donc nécessaire de fournir des outils permettant à ces personnes de comprendre la problématique de la protection de la vie privée et d'appréhender la complexité de cette tâche. Différentes initiatives ont vu le jour dans cette perspective. Des travaux ont proposé d'aider les personnes à comprendre les risques liés à la divulgation de données au travers des jeux sérieux tels que 2025 ex-machina5[19]. Le projet Platform for Privacy Preferences a défini un standard pour uniformiser les politiques en matière de vie privée des sites web afin de permettre aux personnes de comprendre comment les sites web traitent leurs données. Ces politiques sont ensuite évaluées par rapport à des préférences utilisateurs par un mécanisme ad-hoc. Le même objectif est poursuivi par (Kelley et al. 2010). Ils ont remarqué que les gens comprennent les signalétiques nutritionnelles que l'on retrouve sur les emballages d'aliments. Ils ont donc proposé une solution similaire pour représenter les politiques de vie privée. Plusieurs propositions (Inglesant et al. 2008; Shi et al. 2011; Henning 2014) ont présenté des langages naturels contraints pour faciliter la compréhension de politique d'autorisation. Dans la même approche, des travaux proposent des approches pour simplifier les politiques XACML (Stepien et al. 2014; Nergaard et al. 2015). Ces recherches sont nécessaires pour aider les personnes à comprendre les risques qu'elles encourent et à rendre des documents techniques tels que des politiques en matière de vie privée ou encore d'autorisation compréhensibles par le commun des mortels. Cependant, il n'existe que peu de travaux qui aident les personnes à concevoir et écrire des politiques d'autorisation pour protéger leur vie privée. Une première approche pour aider à la conception et l'édition de politique d'autorisation consiste à proposer une interface graphique pour accéder aux différents droits. L'exemple type est le composant privacy guard de la distribution Android cyanogen-mod[20]. Cette interface offre un tableau de bord où sont centralisées les informations relatives à la gestion des droits des applications installées sur le système Android. Il est possible de définir pour chaque application ses droits exacts. Les avantages de cette approche sont 1) l'interface graphique de gestion qui ne nécessite pas de connaissance spécifique à la définition de politique d'autorisation ainsi que 2) la possibilité de gérer finement les droits des applications. Cependant, cette approche ne peut supporter le passage à l'échelle. En effet, elle ne permet d'exprimer que des politiques d'autorisation de bas niveau de type Identity Based Access Control. Pour quantifier le problème, nous avons analysé le nombre moyen de permissions à gérer sur un dispositif d'une application Android. Sachant qu'un smartphone comporte en moyenne 32 applications et que chaque application demande en moyenne 11,4 permissions dont 5,72 ont un impact fort sur la vie privée (nous avons obtenu ces valeurs en analysant les permissions

[19] http://www.2025exmachina.net/jeu

[20] http://www.cyanogenmod.org/

des 50 applications gratuites les plus téléchargées sur Android), un utilisateur doit en moyenne gérer sur son smartphone 364 permissions dont 183 ont un impact direct sur sa vie privée.

Le problème de passage à l'échelle a été traité de manière importante dans les travaux de recherche liés aux modèles de politiques de contrôle d'accès. En effet, les administrateurs ont déjà été confrontés au même problème. Le modèle RBAC (Ferraiolo et al. 1995) par exemple facilite la gestion des permissions en les regroupant par rapport aux rôles que peuvent jouer les utilisateurs dans une organisation. L'abstraction amenée par la notion de rôle limite le nombre de règles. Différents modèles de politique de contrôle d'accès ont proposé des éléments clés à considérer dans le contexte de la gestion de la vie privée ainsi que des abstractions facilitant leur manipulation tels que la finalité d'utilisation d'une ressource (Byun et al. 2005), la sensibilité d'une ressource (Jiang et al. 2002), la confiance (Wagealla et al. 2003), ou encore la précision ou le consentement (Ajam et al. 2010). Ces modèles de politiques de contrôle d'accès offrent la possibilité d'écrire des règles de haut niveau plus adaptées à la gestion d'environnements complexes. Cependant, cette approche nécessite la compréhension des abstractions proposées par les modèles de politiques pour pouvoir les utiliser correctement. Ainsi, une phase de conception est nécessaire avant d'écrire des règles de contrôle d'accès. Imposer ces contraintes à des utilisateurs novices est difficilement envisageable. De plus, créer une interface utilisateur générique permettant d'écrire facilement des politiques manipulant ces concepts abstraits est une tâche très complexe (Graf et al. 2013). Comment éviter l'approche mode novice (simple mais très limité) versus le mode expert (complet mais complexe)?

Partant de ce constat, nous avons proposé une nouvelle approche complémentaire qui permet à un utilisateur novice d'écrire des politiques de haut niveau tout en limitant la charge cognitive nécessaire leur écriture (i.e. phase de conception et interface de spécification). Notre proposition est un système appelé KAPUER (pour Kapuer is an Assistant for the Protection of UsErs' infoRmation) qui utilise les principes issus de l'aide à la décision pour aider les utilisateurs à écrire des règles d'autorisation abstraites. KAPUER analyse les permissions de bas niveau accordées par un utilisateur pour apprendre ses préférences en terme de protection de la vie privée et lui propose des politiques de haut niveau correspondant à ces préférences. KAPUER ne prend pas de décision à la place de l'utilisateur, il l'aide par ses propositions. Ainsi, l'utilisateur peut alors accepter la règle proposée qui sera mise en œuvre par le système d'autorisation, la refuser s'il considère que cette règle n'est pas correcte ou alors la modifier.

6.2 Une courte introduction aux systèmes d'aide à la décision

Les systèmes d'aide à la décision ont été introduits dans les années soixante-dix (Gorry et al. 1971). Cette approche combine des modèles mathématiques pour analyser le comportement des décideurs et des ordinateurs pour leur interactivité et les techniques de visualisation disponibles. Les systèmes d'aide à la décision actuels peuvent aider des utilisateurs à prendre des décisions de plus en plus complexes impliquant beaucoup d'informations.

Un système interactif d'aide à la décision (SIAD en français ou DSS pour Decision Support System en anglais) peut aider les utilisateurs à gérer les prises de décisions complexes en recréant un processus de prise de décision. Afin d'aider le décideur, le système doit avant tout le comprendre. Pour cela, le système et le décideur interagissent l'un avec l'autre. Grâce à ces interactions, le système est capable de proposer de nouvelles solutions à l'utilisateur. Le but principal d'un système d'aide à la décision est d'aider le décideur à prendre des décisions mais en aucun cas les prendre pour lui. Le système est là pour prêter assistance à l'utilisateur et non pas le remplacer.

Il existe plusieurs façons d'aider un utilisateur. Cela peut être en lui expliquant le problème qu'il rencontre, en lui donnant les causes qui ont amené ce problème ou encore en décomposant un problème complexe en plusieurs sous-problèmes plus faciles à appréhender. Par exemple, il existe des tableaux de bord aidant les utilisateurs en agrégeant plusieurs paramètres pour aider à la prise de décision sur les marchés financiers. L'utilisateur est guidé à travers divers indicateurs lui permettant de comprendre les différentes informations disponibles afin de prendre une décision. Une autre manière d'aider le décideur est de lui proposer différentes solutions à son problème. Ce genre de système est appelé un système de recommandation. Amazon, par exemple, utilise un système de ce genre pour proposer à ses clients une liste d'objets potentiellement intéressants en se basant sur leurs anciens achats, leur historique de navigation mais aussi les achats effectués par les autres clients.

Plusieurs aspects doivent être pris en compte pour construire un système de recommandation efficace. Il doit présenter des solutions qui doivent être aussi satisfaisantes que possibles, et ce le plus rapidement possible. Un système où l'utilisateur doit attendre trop longtemps avant d'avoir le choix entre des solutions intéressantes ne sera au final pas ou peu utilisé. Pour comprendre l'utilisateur et lui présenter les meilleures solutions possibles, le système doit interagir avec lui. Ces interactions sont indispensables mais doivent être minimisées. Un système qui solicite trop souvent l'utilisateur ne sera pas non plus utilisé longtemps. La difficulté pour construire un bon système de recommandation est donc de trouver le bon nombre d'interactions nécessaires avant de trouver des solutions satisfaisantes.

Trois approches existent pour construire un système de recommandation (Adomavicius et al. 2005). La recommandation collaborative utilise les informations sur les autres utilisateurs pour trouver les recommandations à faire. Le gros avantage de cette approche est de pouvoir proposer rapidement des solutions à l'utilisateur même sans avoir d'informations sur ses préférences. Etant donné que le système utilise les préférences de tous les utilisateurs, les solutions proposées ne sont pas aussi précises qu'un système n'utilisant que les préférences de l'utilisateur. Les solutions sont trouvées en calculant les similarités et les différences entre les utilisateurs avec par exemple la technique des *k plus proches voisins*.

La deuxième approche est basée sur le contenu et ne prend en compte que les caractéristiques de chaque objet. Par exemple, un film peut être décrit par son titre, sa date de sortie, son réalisateur et ses acteurs. Chaque film peut être décrit par ses caractéristiques et connaître les préférences de l'utilisateur quant à ces caractéristiques peut permettre de faire des recommandations (Cranor et al. 2002).

La dernière approche est une combinaison des deux premières. Cette approche hybride utilise à la fois la recommandation collaborative pour trouver les habitudes des autres utilisateurs et la recommandation basée sur le contenu pour trouver les objets avec des caractéristiques appréciées par l'utilisateur.

Nous pensons que l'approche basée sur le contenu est la plus appropriée pour notre problème pour deux raisons. Tout d'abord d'un point de vue idéologique, nous pensons que le contrôle de la vie privée est quelque chose de personnel. Chaque individu définit ses propres limites par rapport à ce qui pourrait constituer une atteinte à sa vie privée. En effet, ce qui relève de la vie privée est lié à l'affect (Laufer et al. 1977; Smith et al. 2011). Ensuite d'un point de vue technique, l'approche collaborative pose des problèmes quant à la protection des données représentant les préférences utilisateurs et reste une question ouverte aujourd'hui (Jeckmans et al. 2013; Friedman et al. 2015). En effet, il faut des préférences utilisateur précises et détaillées pour qu'un système de recommendation soit efficace. Or plus ces préférences sont précises et détaillées, plus l'utilisateur dévoile des éléments liés à sa vie privée.

Dans un système de recommandation, il est nécessaire de pouvoir évaluer les objets à choisir sur plusieurs critères. En effet, une approche mono-critère n'est pas envisageable car les préférences des utilisateurs sont presque toujours basées sur plusieurs critères. Un système d'aide à la décision a des objectifs concrets. Il n'y a pas d'hypothèses fortes faites sur l'environnement. Simon a proposé pour l'aide à la décision le principe de rationalité limitée (Simon 1972). Les décisions rationnelles sont souvent impossibles à prendre car les critères utilisés pour prendre une décision peuvent être contradictoires. Par exemple, quelqu'un veut acheter une voiture en maximisant la puissance, mais qu'elle soit aussi la plus écologique possible. Une voiture puissante pollue plus qu'une moins puissante, il n'est donc pas possible de maximiser les deux critères. De plus, un décideur humain ne peut pas prendre en compte toutes les conséquences possibles à ses choix car les informations disponibles ainsi que sa charge cognitive sont limitées. Donc plutôt que de choisir la décision optimale, il se retrouve à choisir la plus satisfaisante, c'est à dire la première solution qui lui convient.

Un système de recommandation suit un processus cyclique (Figure 46). Ce cycle commence par une action de l'utilisateur qui peut être un classement de plusieurs objets, donner une note à un ou plusieurs objets ou directement choisir un objet dans une liste. Le système va décomposer l'objet concerné par l'action de l'utilisateur en une liste de critères. Chaque critère est associé à une valeur dépendante de l'action de l'utilisateur. Cette étape est effectuée en utilisant un opérateur de décomposition et une méthode appelée analyse multicritère. Ensuite, cette liste de critères est mise en correspondance avec les préférences actuelles de l'utilisateur. L'ensemble des préférences de l'utilisateur définit le profil utilisateur et est utilisée pour donner un poids à chaque critère de la liste de critères. Le système est alors capable de calculer le score de l'objet en agrégeant tous les critères. Un opérateur d'agrégation est utilisé pour obtenir ce score. Vient ensuite la dernière étape de la phase

d'apprentissage où le système capitalise l'information acquise de l'action de l'utilisateur en mettant à jour le score de tous les critères impliqués en utilisant le score agrégé.

Une fois que les préférences ont été mises à jour, le système peut, avec la même méthode que pendant l'apprentissage, calculer le score de tous les objets. Il décompose les critères et les agrège avec les préférences de l'utilisateur. Une fois que les scores de tous les objets sont disponibles, le système peut les proposer à l'utilisateur et le processus peut recommencer afin d'affiner les recommandations faites à l'utilisateur.

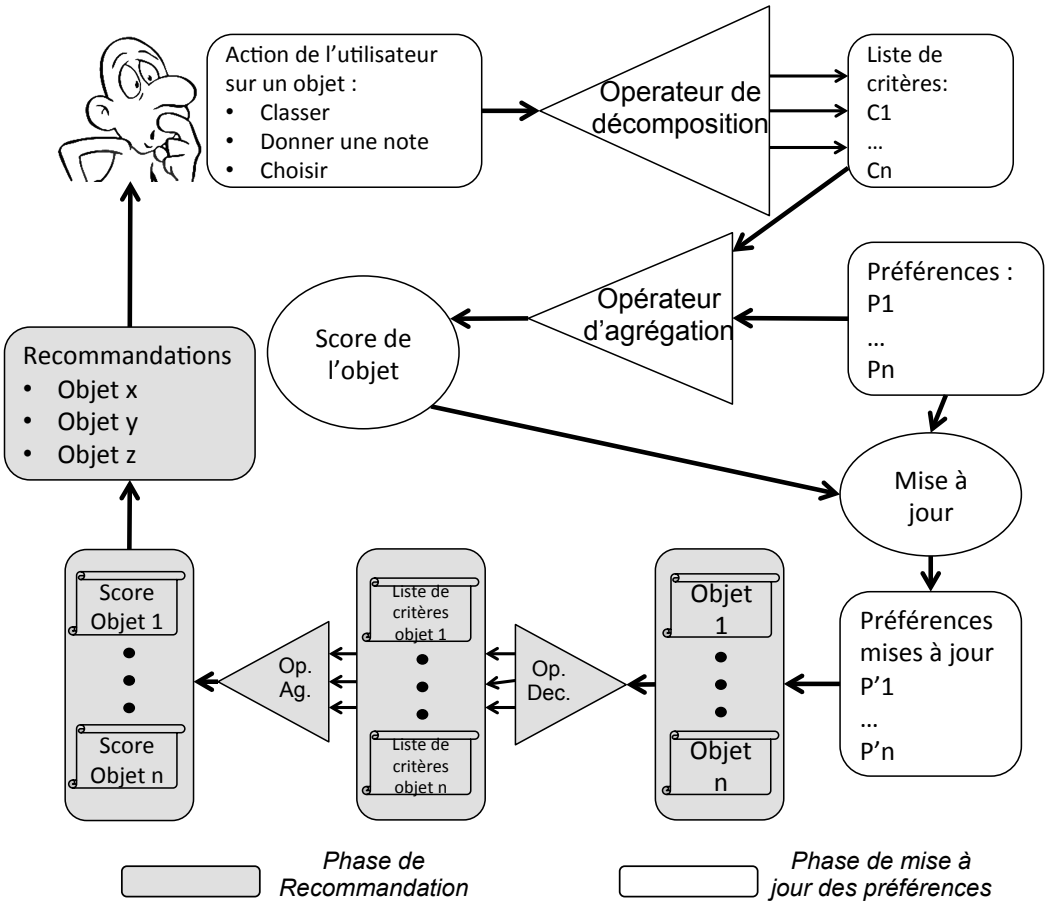


Figure 46. Processus d'un système de recommandation

6.3 Modélisation des critères de préférences pour la protection de la vie privée

Cette section présente la modélisation des critères qui seront utilisés pour calculer les préférences des utilisateurs en terme protection de la vie privée. Cette modélisation est indépendante de tout modèle de politique de contrôle d'accès.

6.3.1 Les critères

Un critère représente l'élément de base constituant une requête d'accès à une ressource protégée. Le critère peut correspondre au nom de l'utilisateur, son âge, le nom de la ressource, le nom

de l'action, etc. Ainsi, *"Jacqueline veut lire le calendrier"* comporte trois critères *Jacqueline*, *lire* et *calendrier*. L'ensemble des critères du système est noté CR. Un critère est composé d'un identifiant et de deux valeurs correspondant aux préférences de l'utilisateur :

- La première, g^t : CR → [0, ∞[représente la préférence de l'utilisateur pour la divulgation d'un critère à l'instant t.
- La deuxième f^t : CR → [0, ∞[représente la préférence de l'utilisateur pour la non-divulgation d'un critère à l'instant t.

Chaque information et critère doivent être notés selon les préférences des utilisateurs. Cette étape constitue le calcul de score. Nous avons choisi d'utiliser une méthode de calcul de score incrémentale uniquement, lors de leur mise à jour, $g^t(x)$ et $f^t(x)$ ne peuvent qu'augmenter, afin d'éviter le problème relatif au manque d'apprentissage. L'apprentissage des préférences se faisant en continu, une valeur élevée de $g^t(x)$ ne veut pas forcément dire que lorsque le critère x est présent, l'utilisateur est fortement enclin à divulguer ses données. Cela peut aussi vouloir dire que ce critère est souvent apparu parmi les requêtes et qu'il a été mis à jour de multiples fois. Pour identifier la signification d'un critère, il faut calculer soit :

- $s^t_D(x)$ correspondant au score du critère x à l'instant t en faveur de la divulgation. Ce score est issu de la différence entre la valeur de divulgation et la valeur de non-divulgation :

$$s^t_D(x) = f^t(x) - g^t(x)$$

- $s^t_{nD}(x)$ correspondant au score du critère x à l'instant t contre la divulgation. Ce score est issu de la différence entre la valeur de non-divulgation et la valeur de divulgation :

$$s^t_{nD}(x) = g^t(x) - f^t(x)$$

Calculés ainsi, les scores $s^t_D(x)$ et $s^t_{nD}(x)$ établissent la position du critère x dans les préférences de divulgation ou non de l'utilisateur. Un faible score de $s^t_D(x)$ et $s^t_{nD}(x)$ reflète une absence claire de raisons justifiant la préférence pour l'une des deux actions. Au contraire, un score élevé de $s^t_D(x)$ ou $s^t_{nD}(x)$ correspond à l'existence de raisons claires confirmant une préférence stricte en faveur d'une des deux actions.

6.3.2 Les classes de critères

Les modèles de politique de contrôle d'accès proposent des éléments clés à prendre en compte dans les politiques tels que :

- la visibilité : Qui veut avoir accès à la ressource (un ami, un collègue, un inconnu, etc.)

- l'aspect temporel : Le moment de la protection (différents jours de la semaine, différentes heures de la journée, etc.)
- l'aspect spatial : Le lieu où se trouve l'utilisateur (chez lui, au travail, etc.)
- la rétention : Comment la ressource est stockée (combien de temps, qui y aura accès, etc.)
- l'intention : Pourquoi la ressource est stockée (à but philanthropique, pour être revendue, etc.)

Pour exprimer ces éléments, nous introduisons la notion de classe de critères. Chaque critère fait partie d'une classe de critères par la relation *Association Criterion Class* $ACC \subseteq CR * C$ où l'ensemble des classes de critères est noté C. Le système étant générique, les classes de critères ne sont pas fixées et n'importe quelle classe de critères peut être créée. Pour simplifier notre notation par la suite, nous définissons la fonction class qui renvoie l'ensemble des critères appartenant à une même classe :

$$class : C \rightarrow \wp^{CR}$$
$$x \mapsto \{y \in CR \mid (y, x) \in ACC\}$$

6.3.3 Les méta-critères

Nous définissons la notion de *méta-critère* pour représenter les abstractions des modèles de politique de contrôle d'accès comme le rôle de RBAC (Ferraiolo et al. 1995), les vues/activités de OrBAC (Ajam et al. 2010), les hiérarchies d'intentions de PRBAC (Byun et al. 2005), etc. Un méta-critère est un critère ayant un niveau d'abstraction supérieur à un ou plusieurs critères appartenant à la même classe. L'ensemble des méta-critères du système est noté MCR, cet ensemble est inclus dans CR. Un méta-critère permet de regrouper plusieurs critères partageant une caractéristique commune. Par exemple, considérons les critères « Jacqueline » et « Bernard ». Ces deux critères ont une caractéristique commune: être des parents. On peut ainsi définir le méta-critère "Parent" regroupant les critères « Jacqueline » et « Bernard ». De même, le méta-critère « Famille » est un niveau d'abstraction supérieur à « Parent ». Les valeurs $f^t(x)$ et $g^t(x)$ du méta-critère *x* lui sont propres.

Un méta-critère étant aussi un critère, il est possible pour chaque classe de critères cl de créer une hiérarchie $H_{cl} \subseteq CR * MCR$ entre ces critères tel que $\forall(c_1,c_2) \in H_{cl}$, $class(c_1) = class(c_2)$ (cf. Figure 47).

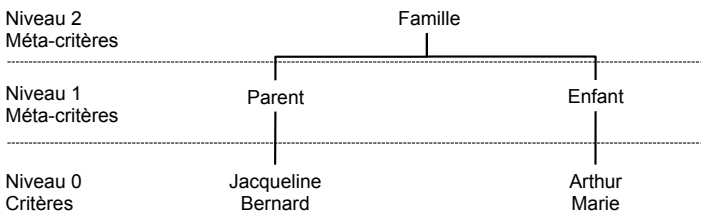


Figure 47. Hiérarchie de méta-critères

6.3.4 Les groupes de critères

Afin de pouvoir analyser les relations inter-critères qui permettent de capter plus finement les préférences des utilisateurs, nous définissons le *groupe* de critères. Un groupe de critères est une association de *n* critères. Un groupe de critères a ses propres valeurs, indépendantes des valeurs des critères qui le composent. Les critères ou méta-critères composant un groupe de critères doivent appartenir à des classes de critères différentes. Ainsi prenons par exemple les critères « Parent » et « Calendrier » appartenant à deux classes différentes, nous pouvons créer le groupe de critères {Père, Calendrier}. L'ensemble des groupes de critères G est défini par :

- L'ensemble G est compris dans l'ensemble des parties de CR: $G \subseteq \wp^{CR}$
- Un groupe de critères est composé au minimum de deux critères.

$$\forall g \in G, |g| \geq 2$$

- Deux critères d'un même groupe ne peuvent appartenir à la même classe de critère.

$$\forall g \in G, \forall (c_1,c_2) \in g \times g, c_1 \neq c_2 \Rightarrow class(c_1) \neq class(c_2)$$

La Figure 48 illustre les concepts de critère, classe et groupe dans laquelle nous considérons trois classes correspondant à Qui (bleu), Quoi (Rouge) et Où (Vert).

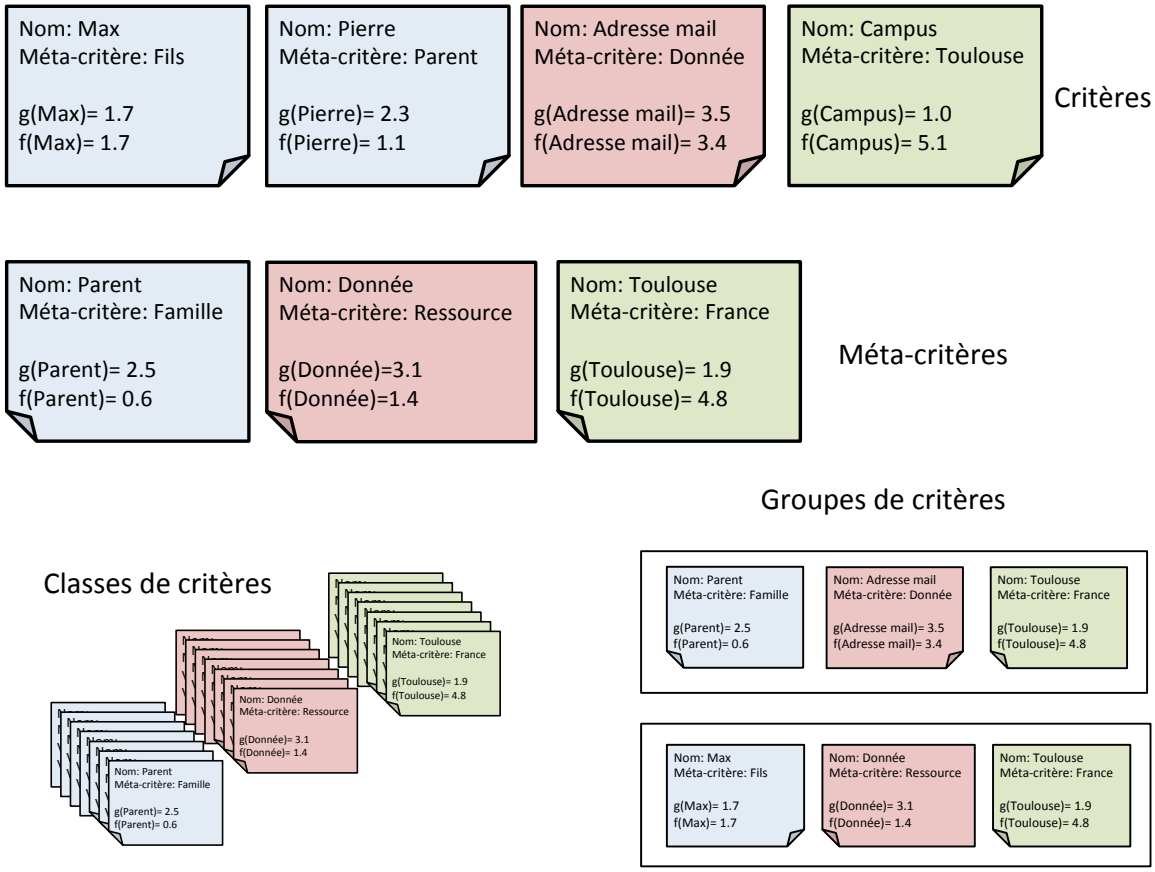


Figure 48. Illustration des notions de critère, classe et groupe

6.4 Intégration d'un système de recommandation dans XACML

Nous avons intégré le système de recommandation dans le système de gestion d'autorisation XACML de part la modularité de l'architecture et l'approche ABAC qui est assez similaire à l'approche critère utilisée dans les SIADs. La Figure 49 présente les interactions entre les entités PEP/PDP de XACML (grisé dans la figure) et le SIAD (en blanc dans la figure).

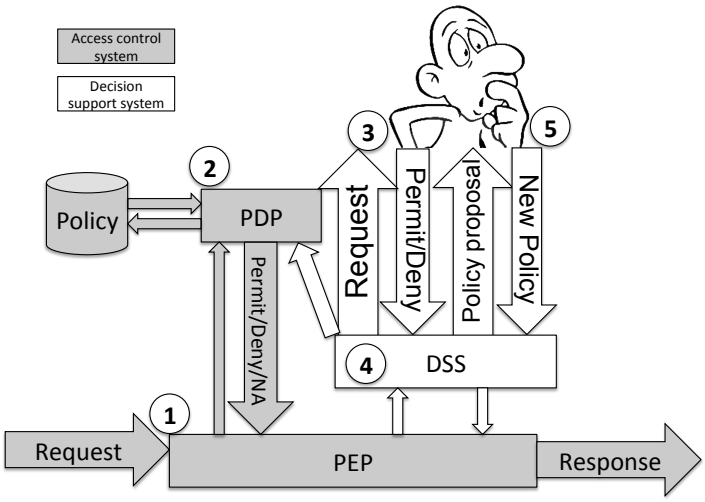


Figure 49. Intégration du SIAD avec XACML

Etape 1 : Capture et traduction d'une requête d'accès en XACML

Lorsqu'une requête arrive, elle est interceptée par le PEP. Son rôle est de traduire la requête sous forme d'attributs utilisé dans l'approche pour l'envoyer au PDP, et d'appliquer la décision qui est prise concernant la requête. Le système est générique et il est possible d'utiliser et de transformer n'importe quelle information disponible dans la requête sous forme d'attributs. Les requêtes sont traduites selon les informations qu'elles contiennent ou que le PEP peut obtenir via d'autres bases d'informations (tels que le carnet d'adresse, etc). La traduction d'une requête d'accès est un document XML regroupant les attributs sous les balises sujet, ressource, action et environnement. Cette requête est ensuite transmise au PDP qui va continuer le processus de contrôle d'accès.

Etape 2 : Analyse de la requête par rapport aux politiques de sa base

Lorsque le PDP reçoit une requête XACML contenant un ensemble de couple <identifiant d'attributs, valeur>, il peut évaluer certaines règles de cette politique. Dans le cas où les attributs et valeurs des attributs de la requête correspondent à ceux d'une règle, la valeur de la règle de cette politique est retournée au PEP. Une règle peut prendre deux valeurs, "PERMIT" si la requête est acceptée, "DENY" si elle est refusée.

Dans le cas où les attributs et valeurs des attributs de la requête ne correspondent à aucune des règles présentes dans la politique, la décision "NOT APPLICABLE" est renvoyée au PEP. Le PDP n'a

pas pu prendre de décision basée sur la politique existante. Nous utilisons cette décision pour interagir avec l'utilisateur.

Etapes 3 et 4 : Interactions avec l'utilisateur pour apprendre ses préférences

C'est à cette étape qu'intervient notre système d'aide à la décision. La décision "NOT APPLICABLE" indique qu'il n'y a pas de règles d'autorisation correspondant à une requête donnée. Il serait envisageable de demander à l'utilisateur d'écrire via une interface graphique une règle d'autorisation. Cependant ce choix nécessiterait une phase de conception de la part de l'utilisateur pour écrire une règle utilisant des concepts abstraits : il devrait prendre une décision complexe.

Nous préférons lui demander de prendre une décision plus simple qui est limitée à cette requête précise. La Figure 50 est une copie d'écran d'un exemple d'interaction avec l'utilisateur dans le cadre de systèmes mobiles Android. Le système informe l'utilisateur qu'une entité (l'application "fr.irit.tests") veut accéder à une ressource (sa liste de contacts) et lui demande s'il accepte de partager cette ressource. Nous utilisons cette interaction pour apprendre les préférences de l'utilisateur. Deux actions sont donc présentées à l'utilisateur, la divulgation *D* et la non divulgation *nD*. Une fois que l'utilisateur a répondu, le couple (requête, action) est envoyé au système d'aide à la décision qui l'analyse et utilise l'information pour faire évoluer les préférences de l'utilisateur. Les préférences de l'utilisateur sont une représentation, par un ensemble de critères, de la politique de confidentialité préférée par l'utilisateur. La notion d'attribut dans XACML étant très proche de celle de critère tel que nous l'avons défini, il est possible de transformer une requête en une liste de critères.

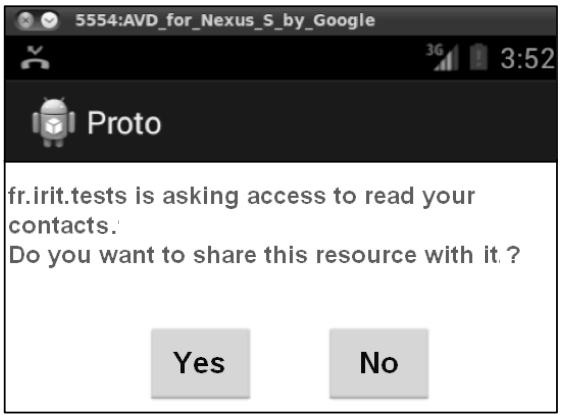


Figure 50. Exemple d'interaction avec l'utilisateur lors de la phase de mise à jour des préférences

Le SIAD fait ainsi un apprentissage continu de ces préférences afin d'être au plus proche de la politique de confidentialité voulue par l'utilisateur. Ainsi dans notre cas, une décision "NOT APPLICABLE" indique que le SIAD doit parfaire l'apprentissage des préférences de l'utilisateur et pour cela, il informe l'utilisateur de la requête en cours et lui demande de prendre une décision par rapport à la divulgation ou non de la donnée de vie privée concernée. Cette interaction permet de mettre à jour les valeurs des critères de la requête ainsi que leurs méta-critères et donc d'affiner les préférences de l'utilisateur. Lorsque le SIAD aura une connaissance suffisante des préférences de l'utilisateur, il pourra lui proposer l'ajout d'une règle d'autorisation (étape 5).

Etape 5 : Propositions de politiques abstraites à l'utilisateur

L'objectif principal de KAPUER est de faire des propositions de règles d'autorisation abstraites à l'utilisateur. Cependant, il ne doit pas proposer n'importe quelle règle. Tout d'abord, la règle doit être de haut niveau afin qu'elle couvre un nombre de requêtes d'accès important. Cela permet d'éviter un nombre trop important de règles de bas niveau qui seraient difficilement gérables ensuite par l'utilisateur et retrouver les mêmes difficultés qu'un système comme cyanogen-mod. De plus, définir rapidement des règles de haut niveau limite le nombre d'interactions avec l'utilisateur. Le deuxième point est de proposer des règles qui conviennent à l'utilisateur. Si le système propose des règles « hors sujet », l'utilisateur sera enclin à ne plus utiliser le SIAD.

Faire une proposition à l'utilisateur revient à déterminer que l'action associée à cette proposition est strictement préférée à son contraire. Autrement dit, soit l'utilisateur préfère autoriser la divulgation, soit il préfère la refuser. Si le système n'est pas en mesure de faire une proposition, c'est qu'il n'y a pas de préférence entre les deux actions. Deux situations peuvent entraîner cette non-préférence:

- la première lorsque le système n'a pas une représentation précise du comportement de l'utilisateur, donc quand il manque d'information.
- la deuxième lorsque l'utilisateur n'a pas un comportement fixe et n'agit pas de la même façon à chaque fois. Dans ce cas, le système ne peut pas inférer le comportement de l'utilisateur ni lui proposer une règle.

Afin de gérer les préférences, nous utilisons un système relationnel parfait de préférences (Giard et al. 1985). Il est constitué des deux relations binaires transitives suivantes:

- l'indifférence ~ ou non-préférence qui correspond à une absence de raisons qui justifieraient une préférence en faveur d'une action ou de l'autre:

$$\sim : a \sim a' \Leftrightarrow a \, I \, a'$$

I étant une relation symétrique réflexive.

- la préférence stricte $\succ$ qui correspond à l'existence de raisons justifiant la préférence en faveur d'une des deux actions:

$$\succ : a \succ a' \Leftrightarrow a \, P \, a'$$

P étant une relation asymétrique irréflexive.

Lorsque le SIAD reçoit une requête et l'action prise par l'utilisateur, le système effectue une analyse de ce couple. Pour cela nous utilisons une méthode appelée analyse multicritère (Bouyssou et al. 2006). Chaque requête est décomposée en critères, ces critères sont ensuite agrégés grâce à un opérateur d'agrégation. Les préférences de l'utilisateur sont utilisées pendant cette étape pour pondérer les critères. Le résultat de l'agrégation fournira un score S_R^t de la requête R, évaluant le degré de

connaissance des préférences de l'utilisateur face à cette requête. Avec ce score et la décision de l'utilisateur, le système peut mettre à jour les valeurs des critères de R et de leurs méta-critères.

Afin de savoir si une proposition correspond à une préférence stricte, le système doit calculer le score S_R^{t+1} de la requête avec les valeurs $f^{t+1}(x)$ et $g^{t+1}(x)$ des critères et méta-critères mis à jour. Ce nouveau score est ensuite comparé à un paramètre λ, correspondant à la valeur seuil entre la relation d'indifférence et de préférence stricte. Si S_R^{t+1} est inférieur à λ, nous nous trouvons dans une situation d'indifférence et aucune proposition ne sera faite à l'utilisateur. Si S_R^{t+1} est supérieur à λ, nous nous trouvons dans une situation de préférence stricte et la proposition peut être présentée à l'utilisateur. λ est un paramètre qui influe sur la vitesse de proposition à l'utilisateur. Plus il est faible, plus le système fait des propositions à l'utilisateur rapidement. Inversement, plus il est élevé, plus le système est lent à faire des propositions à l'utilisateur.

Dans le cas où S_R^{t+1} est supérieur à λ, le système propose une nouvelle règle à l'utilisateur. Cela correspond à une nouvelle interaction avec lui. Durant cette interaction, le système propose à l'utilisateur d'insérer dans la base de politiques une nouvelle règle, dont les attributs correspondent aux critères ou méta-critères de la proposition. La décision de cette règle est aussi communiquée à l'utilisateur. Le choix est donné à l'utilisateur d'accepter cette règle ou de la refuser.

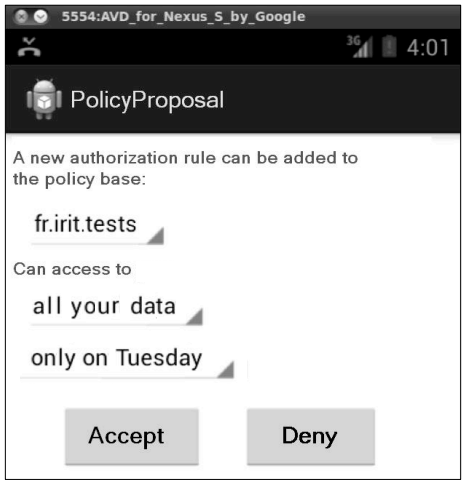


Figure 51. Exemple de proposition de règle à l'utilisateur

Bien que les attributs présentés à l'utilisateur soient censés être pertinents pour lui, celui-ci peut malgré tout modifier chaque attribut de la règle proposée. Soit l'attribut représente un critère et l'utilisateur peut choisir un méta-critère pour obtenir une règle plus agrégée. Soit l'attribut représente un méta-critère et l'utilisateur peut choisir le critère de la requête s'il ne veut pas que la règle soit agrégée avec ce méta-critère. La Figure 51 présente un exemple de proposition de règle à l'utilisateur. Ici la règle présentée à l'utilisateur lui propose d'accepter de partager sa liste de contact tous les mardi avec l'application "fr.irit.tests". Le système propose ici une règle dont l'abstraction a pu être déterminée sur la ressource et l'aspect temporel. L'utilisateur peut modifier les attributs pour que la

règle soit étendue par exemple à toutes les applications ou à tous les jours de la semaine. Ainsi, l'utilisateur peut construire une règle lui convenant, sans avoir besoin de la spécifier et de l'écrire.

Si l'utilisateur accepte cette règle, le SIAD la transforme en XACML et l'ajoute dans la base de politiques du système de contrôle d'accès avant de communiquer la décision au PEP. S'il refuse, seule la décision est transmise au PEP. Une fois que le PEP reçoit la décision correspondant à la requête, elle est traduite pour être comprise par l'entité ayant fait la demande puis envoyée.

6.5 Apprentissage des préférences relatives à la vie privée

L'apprentissage des préférences utilisateur doit être le plus rapide possible. De plus, le nombre d'interactions entre le SIAD et l'utilisateur doit être aussi limité que possible afin de ne pas surcharger l'utilisateur de questions. L'utilisation des méta-critères pour agréger les politiques est un moyen de baisser ce nombre. Cependant, ce facteur n'est pas suffisant. Le nombre d'interactions dépend aussi des préférences apprises et de la vitesse à laquelle le SIAD les apprend. L'agrégation des critères pour calculer le score d'une requête et la mise à jour des critères sont les deux étapes qui influent le plus sur la vitesse d'apprentissage. Nous avons testé trois opérateurs d'agrégation différents:

- la moyenne pondérée, un opérateur utilisé dans la majorité des SIAD pour sa simplicité. Chaque critère est évalué indépendamment.
- l'intégrale de Choquet (Grabisch et al. 2000), un opérateur plus complexe qui utilise l'importance de chaque critère et les interactions entre eux pour avoir un meilleur apprentissage. Nous avons utilisé Kappalab (Grabisch et al. 2006), un plug-in de R pour mettre en place nos intégrales de Choquet.
- notre propre opérateur, Kagop (Kapuer AGgregation OPerator) (Oglaza et al. 2014), qui se place entre la moyenne pondérée et l'intégrale de Choquet. En plus des critères de la requête, il utilise tous les groupes de critères. Nous utilisons cet opérateur pour voir si les groupes de critères peuvent aider le système à trouver des interactions entre plusieurs critères.

Afin de pouvoir obtenir suffisamment de données pour pouvoir comparer les différentes approches d'apprentissage, de nombreux utilisateurs et périphériques sont nécessaires. Pour passer outre ces contraintes, nous avons développé un simulateur. Ce simulateur permet deux choses. Tout d'abord, il est possible de le configurer avec un ensemble de critères sur plusieurs classes ainsi qu'une hiérarchie pour chacune des classes afin qu'il puisse générer un nombre important de requêtes en choisissant aléatoirement un critère de chaque classe. Ceci permet de simuler des requêtes d'accès. Ensuite, il permet de simuler le comportement d'un utilisateur via un ensemble de règles d'autorisation. Ainsi, lorsque le SIAD demande une interaction lors de sa phase d'apprentissage, le simulateur répond automatiquement par accepter ou refuser selon ces règles. De la même manière, chaque fois que le SIAD fait une proposition de règle, le simulateur compare cette proposition avec sa liste de règles.

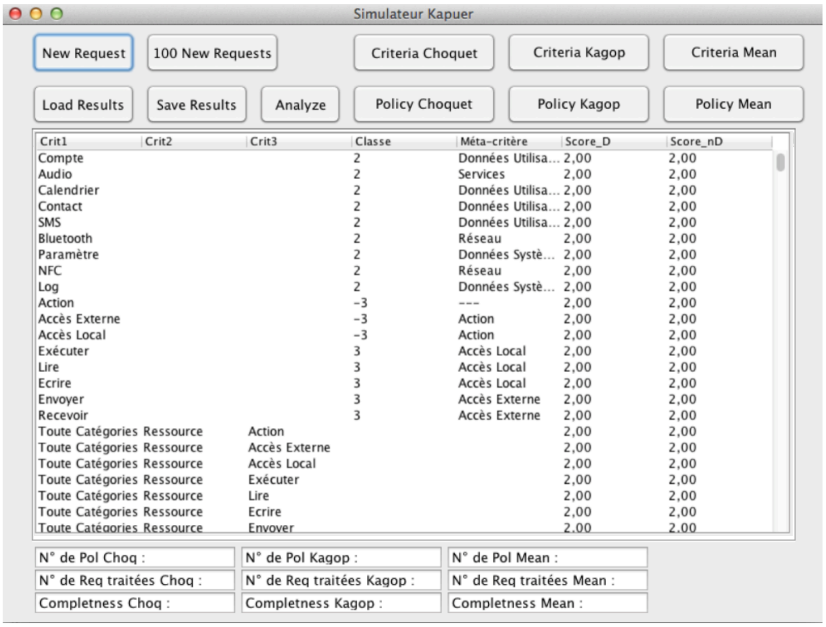


Figure 52. Ecran du simulateur

Pour permettre une comparaison des algorithmes d'apprentissage, nous avons défini les métriques suivantes :

- Le nombre de règles d'autorisation créées pendant la simulation.
- Le nombre d'interactions nécessaires pendant la simulation.
- Le pourcentage de complétude, c'est à dire le pourcentage de requêtes que le système peut gérer grâce aux règles d'autorisation créées pendant la simulation. Nous avons aussi regardé l'évolution de cette complétude afin de déterminer combien de requêtes sont nécessaires pour arriver à différents seuils de complétude.
- Le taux d'erreurs dans les propositions. Le système peut proposer des règles d'autorisation contraires aux règles de comportement mais aussi des règles d'autorisation trop abstraites et donc partiellement erronées.

Chacun des trois opérateurs d'agrégation a été testé sur deux scénarios :

- le premier utilisant une base de critères réduite et des hiérarchies de critères limitées à un seul niveau d'abstraction
- et le deuxième utilisant une base de critères plus large et des hiérarchies de critères sur plusieurs niveaux.

Les résultats ont confirmé que dans ce problème d'aide à la décision multicritère, il y a interaction entre les critères. De ce fait, la méthode utilisant la moyenne pondérée n'obtient pas de bons résultats. Pour arriver à recréer la politique d'autorisation, elle a besoin de plus d'interactions et de plus de règles. Par contre les règles proposées sont pertinentes et l'apprentissage ne fait pas d'erreurs. Les deux autres opérateurs d'agrégation partaient avec un avantage vu qu'ils prennent en

compte les interactions entre les critères. Pour l'intégrale de Choquet, la formule de mise à jour des méta-critères est dépendante de la base de critères, des hiérarchies et du comportement de l'utilisateur. Ainsi, l'algorithme a dû être paramétré différemment pour chaque scénario afin d'arriver à des résultats convenables. Hors il est impensable de demander à l'utilisateur de devoir paramétrer le système avant de l'utiliser. Kapuer est destiné à être utilisé par tout type d'utilisateurs et doit pouvoir fournir des résultats satisfaisant quel que soit le profil de l'utilisateur. Finalement, nous avons pu montré que Kagop, l'opérateur d'agrégation que nous avons proposé, est l'opérateur qui obtient les meilleurs résultats. De plus, ils sont stables sur toutes les simulations. Cette méthode est utilisable aussi bien sur une base de critères réduites qu'une base large et les règles d'autorisation propose plus d'abstractions que les autres méthodes permettant ainsi de recréer la politique d'autorisation de l'utilisateur avec moins d'interactions et moins de règles d'autorisations. L'effort de l'utilisateur est ainsi minimisé.

Nous avons aussi comparé l'effort demandé par Kapuer par rapport aux autres solutions déjà existantes et plus particulièrement CyanogenMod qui utilise une interface graphique, facile à utiliser et accessible à tous. Pour cela, Nous avons compté le nombre de pressions du doigt nécessaires pour recréer chaque règle de comportement. Lorsque Kapuer est implémenté sur un smartphone, les interactions avec l'utilisateur sont aussi effectuées avec une pression du doigt. Comparer le nombre de pressions est donc valable pour évaluer l'effort nécessaire pour chaque méthode. Sur notre deuxième scénario qui consiste en 8 règles autorisations abstraites portant sur les 50 applications gratuites les plus téléchargées sur Android, la différence est flagrante avec 190 pressions pour Kapuer contre 848 pour CyanogenMod. Ceci nous prouve que l'utilisation des SIADs pour la gestion des autorisations est une approche intéressante.

6.6 Bilan

Initialement, mes travaux de recherches avaient pour objectif d'offrir des solutions de gestion de la sécurité à des entreprises ou plus généralement à des organisations réelles ou virtuelles (Cf. Chapitre 2). Par conséquent, il était concevable de prendre comme hypothèse qu'il existe au moins un administrateur/ingénieur qualifié dans le domaine de la sécurité. Dans le domaine de la protection de la vie privée, cette hypothèse est fausse. L'utilisateur du système de gestion peut être n'importe quelle personne. C'est pourquoi il nous a fallu réfléchir à une autre approche pour l'édition de politique afin de couvrir la phase de spécification de politiques d'autorisation (Figure 53).

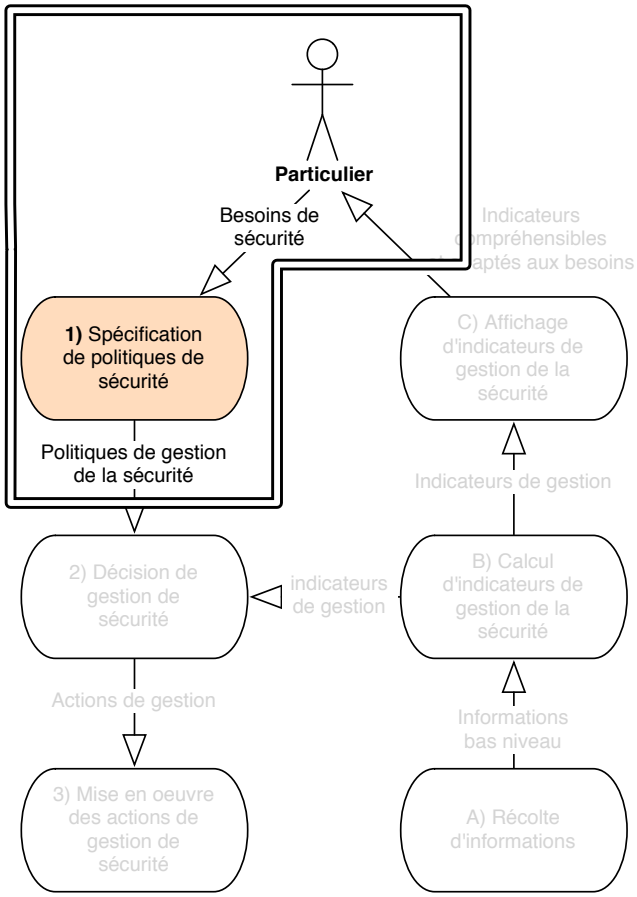


Figure 53. Eléments de la boucle de gestion traités dans le chapitre 6

Ce travail a été initié dans le cadre de l'axe stratégique Systèmes Socio Techniques Ambiants de l'IRIT. J'ai plus particulièrement participé au groupe de travail portant sur la notion de contexte et qui est animé par Thierry Desprats. Les intervenants du groupe provenant de différentes équipes de l'IRIT ayant différentes problématiques de recherche liées à ce concept, nous avons pu étudier la notion de contexte avec différents points de vue, ce qui fut très enrichissant. C'est dans cet environnement que j'ai rencontré Pascale Zaraté qui travaille sur les systèmes d'aide à la décision. Nous avons alors eu l'idée de travailler sur un système d'aide à la décision pour la gestion des autorisations. Cette idée a pu se concrétiser par la suite lors d'une thèse co-encadrée et dans la participation au projet ANR INCOME.

Il existe encore de nombreux défis à relever dans l'apprentissage des préférences en terme de protection de la vie privée à résoudre. Tout d'abord, la vitesse d'apprentissage de l'approche basée sur le contenu peut être largement accélérée avec une phase d'initialisation. Nous avons tenté de faire un questionnaire qui aurait pu être rempli par l'utilisateur au moment de l'initialisation du système. Cependant, un test de ce questionnaire a été effectué sur un panel d'utilisateurs (26 étudiants du master droit informatique à l'UT1) et nous a démontré que nos questions n'amenaient pas assez d'information. Une deuxième difficulté réside dans l'apprentissage des exceptions et/ou des changements de comportements de l'utilisateur par rapport à des propositions acceptées. Nous

pourrons rechercher des solutions du côté des systèmes d'apprentissages adaptatifs comme par exemple (Gama et al. 2014).

Chapitre 7. Conclusion et perspectives de recherche

7.1 Conclusion

Durant ces quinze dernières années, les entreprises ont ouvert leurs infrastructures informatiques au monde extérieur afin de pouvoir répondre aux besoins de collaboration, de mobilité de leurs employés, et d'externalisation de leurs services informatiques, etc. On parle de transformation numérique qui impacte les modèles métiers des entreprises. Selon certaines prévisions, la future décennie sera marquée par l'intégration des réseaux sociaux, de la mobilité, des outils d'analyse, du cloud computing et de l'internet des objets. On retrouve plusieurs termes pour exprimer ce changement comme *the nexus of forces* (OpenGroup 2014) ou encore l'acronyme SMACT (Bloem 2014). Cette évolution a pour conséquence de changer le périmètre à protéger. En effet, celui-ci ne se limite plus uniquement au réseau physique de l'entreprise. L'information et les personnes sont devenues le nouveau périmètre à sécuriser (Harkins 2012) qui est donc beaucoup plus dynamique, imprécis et complexe. En même temps, les attaques de sécurité menées par un hacker isolé en quête de gloire ont été remplacées aujourd'hui par des attaques ciblées perpétrées par des groupes bien organisés (Interpol 2015). Ainsi, l'objectif des équipes de cybersécurité est double : rendre possible et protéger (Harkins 2012). Pour rendre possible, la protection du capital numérique doit être adaptable, flexible et dynamique pour à la fois permettre à l'entreprise de se développer mais elle doit aussi de se prémunir contre de nouvelles menaces. Les projets actuels de gestion des identités et des accès se posent donc la problématique de permettre aux bonnes personnes d'accéder aux bonnes ressources dans les bonnes conditions (au bon moment, bon endroit, bonne situation, etc). Dans ce manuscrit, j'ai décrit mes travaux de recherche effectués durant ces dix dernières années. Sous différents angles, ils ont tous traité de cette problématique de gestion de la sécurité de ces environnements qui sont de plus en plus virtuels et ce avec comme dénominateur commun : exprimer les politiques de sécurité sous forme de contraintes sur des attributs et les déployer en suivant l'architecture de gestion à base de politiques.

Dans le cadre de ces recherches, j'ai co-encadré six thèses qui ont été soutenues plus deux autres sont en cours. La Figure 54 montre les noms des docteurs/doctorants encadrés avec la date de soutenance ainsi que le périmètre couvert par leur thèse dans notre boucle de gestion de la sécurité. Initialement, nous portions notre attention particulièrement sur la gestion de la sécurité pour des organisations. Les collaborations entre organisations évoluant, nous avons traité des problématiques de domaines d'administration multiples et de partage d'identités (Kamel 2008), d'analyse formelle de

mesures de sécurité (El Khoury 2014), de dynamicité des droits d'accès (Kabbani 2015) et par extension de dynamicité de la gestion (Cheaito 2012). Ceci vient du fait qu'avant mon arrivée en thèse, une partie des activités de recherche de l'équipe SIERA se concentraient sur la gestion de la sécurité réseau. Mes travaux de thèse puis mon expérience en post-doc ont orienté cette thématique vers la gestion de la sécurité des services informatiques de manière plus globale. En marge, nous avons entrepris des travaux portant sur la protection des particuliers. Les besoins de mécanismes de sécurité pour favoriser la protection de la vie privée ont été perçus par la communauté de recherche et, aujourd'hui, un nombre important de projets traite de ce sujet. Dans ce paysage, notre approche est originale car elle consiste à voir chaque personne comme l'administrateur de son propre réseau. Ainsi, notre idée n'est pas de lui proposer un outil particulier pour une application particulière mais de lui offrir des outils pour qu'il ait une vue éclairée de la problématique de la sécurité et qu'il puisse prendre des décisions de sécurité informées. C'est avec cette vision que nous avons travaillé sur la construction d'indicateurs représentant la qualité des certificats X.509 (Wazan 2011) ou encore un système d'aide à la décision pour écrire des politiques d'autorisation (Oglaza 2014).

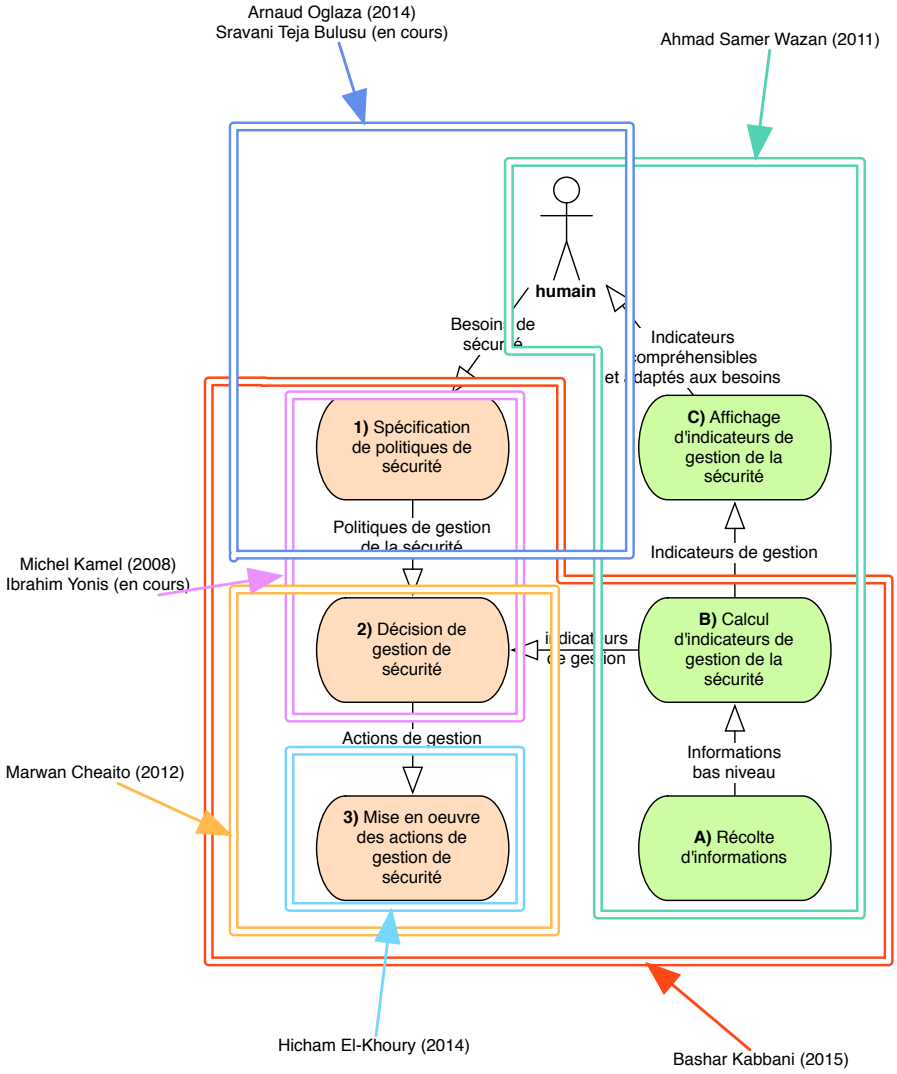


Figure 54. Distribution des thèses coencadrées

7.2 Perspectives de recherche

Mon projet de recherche est dans la continuité de mes travaux actuels. Il est articulé autour de trois axes : la gestion dynamique de la sécurité, l'expression et l'analyse de la sécurité, et enfin la gestion de la sécurité pour les particuliers. Les sections suivantes présentent quelques éléments de prospective dans chacun de ces trois axes.

7.2.1 Vers une gestion dynamique de la sécurité

Le premier axe de recherche que je souhaite continuer à développer porte sur le dynamicité de la sécurité et donc de sa gestion. En effet, les besoins d'accès aux services IT à toute heure, à partir de n'importe quel endroit, depuis tout support impose une dynamicité accrue de la sécurité.

Pour appréhender cette dynamicité de l'environnement géré nous avons eu besoin de nous reposer sur un élément stable à travers le concept de situation. Pour cela, nous avons décrit un cadre de gestion de la sécurité orienté par les situations. Ce concept est l'élément clé de notre solution. Dans le futur, je veux approfondir ce concept sur deux aspects : l'expression/validation et l'identification.

Tout d'abord, nos récents travaux ont mis en avant l'existence de situations avec différents niveaux d'abstraction. De plus, il existe des dépendances entre ces situations. Prenons par exemple la situation d'un poste de travail et la situation du réseau de l'entreprise, le changement de situation du poste de travail peut avoir un impact sur la situation du réseau de l'entreprise. Nous devons donc améliorer ce point en regardant les travaux dans le domaine de l'intelligence artificielle et l'informatique pervasive qui ont étudié cette problématique à la fois en terme de modélisation (Costa et al. 2006) mais aussi d'analyse formelle (Denecker et al. 2007; Boytsov et al. 2013). Nous pourrons ainsi formaliser et valider des politiques de sécurité orientées par les situations.

L'approche d'identification de situation que nous avons suivie est de type spécification (Ye et al. 2012) où un expert décrit les situations au travers de règles. Actuellement, les situations sont écrites dans le formalisme Esper Event Processing Language (EsperTech 2015). Si ce langage est puissant pour exprimer des contraintes temporelles, ce langage ne permet pas de représenter l'incertitude. Il serait intéressant d'intégrer nos travaux sur la gestion de la confiance dans l'identification des situations. Un autre problème est le passage à l'échelle. Plus nous intègrerons de capteurs, plus il sera compliqué pour l'expert d'écrire ces règles du fait de la diversité des données et des source de données. Il est donc nécessaire de proposer un cadre pour faciliter l'expression de ces règles en prenant en compte ce facteur d'échelle. Une approche possible serait de compléter notre identification de situation basée sur la spécification par une identification basée sur l'apprentissage (Ye et al. 2012).

Améliorer la dynamicité de la sécurité implique obligatoirement d'offrir en parallèle des outils de gestion de cette sécurité qui soient eux aussi dynamiquement adaptables. Je pense que les travaux sur le déploiement de logiciel autonome (Arcangeli et al. 2015), qui proposent des solutions pour gérer

automatiquement le cycle de vie du déploiement d'un logiciel distribué et ce selon différents critères, représentent une piste très intéressante à suivre.

Enfin, les travaux sur le chiffrement homomorphique (Gentry 2009) ont permis de nouvelles utilisations sur le traitement sur des données chiffrées avec les circuits brouillés (Huang et al. 2011) ou les machines de Turing aveugles (Rass 2013). De même, le chiffrement basé sur les attributs (Sahai et al. 2005) permet de faire du contrôle d'accès cryptographique sur des données avec des autorités multiples (Chase et al. 2009). Plusieurs propositions ont montré l'intérêt de cette approche pour le contrôle d'accès aux données en particulier stockées dans les nuages informatiques (Lounis et al. 2016; Jung et al. 2015).

7.2.2 Vers une gestion dynamique et contrôlée de la sécurité

Offrir des outils de gestion dynamique de la sécurité n'est pas suffisant. Il faut aussi garantir que les mesures de sécurité mises en œuvre sont correctes vis à vis d'exigences de sécurité mais aussi ne rentrent pas en conflit avec les mesures déjà existantes. Cette analyse doit être automatisable et potentiellement réalisée au moment de la prise de décision des actions de gestion. De plus, il faut que la définition des exigences de sécurité considère la dynamique de l'environnement géré.

La phase amont de définition des exigences (l'élicitation, la représentation et l'analyse des exigences) m'intéresse particulièrement car elle traite à la fois d'aspects techniques mais aussi humains. En effet, la phase de définition des exigences nécessite de mettre d'accord différentes personnes et donc les outils de définition d'exigences doivent être un outil de communication entre personnes ayant des connaissances et des points de vue différents. Quelques documents de standardisations comme NIST 800-160 (Ross et al. 2014) proposent de structurer ce processus. Des méthodes et outils ont été proposés par la communauté de chercheurs (Uzunov et al. 2012). Les approches d'ingénierie des exigences orientées par les buts (Regev et al. 2005) telles que KAOS (Van Lamsweerde 2009) ou I*/TROPOS (Giorgini et al. 2005) possèdent à la fois un langage graphique et un langage formel. Ces approches permettent d'analyser les besoins de sécurité par l'introduction de menaces (anti-buts pour KAOS ou menaces pour Secure TROPOS) mais aussi en validant ce qui est exprimé (via des solveurs SAT pour KAOS ou Answer Set Programming pour i*/Secure TROPOS). Cependant, ces approches sont peu utilisées dans l'industrie.

Dans le cadre du projet IREHDO2 qui vient de commencer, nous avons la chance de pouvoir discuter avec des personnes chargées de la sécurité et qui interviennent à différentes étapes de la définition et validation des exigences de sécurité. De ces premières discussions, j'ai pu me rendre compte qu'il n'existe pas une seule et unique technique d'analyse de risque adaptée à tous les besoins. De même, selon la partie prenante et le moment où elle intervient dans le processus de définition des exigences, l'approche pour exprimer les exigences la plus adaptée n'est pas la même (orientée agent comme TROPOS (Giorgini et al. 2005), orientée par les objectifs comme KAOS (Van Lamsweerde

2009) ou encore orientée par des patrons comme les *security problem frames* (Hatebur et al. 2006)). Il faut donc trouver une solution qui permette d'intégrer cette diversité d'outils et de techniques.

7.2.3 Vers une gestion de la sécurité pour tous les usagers

Pour terminer, le dernier axe de recherche que je veux continuer à traiter est celui de la gestion de la sécurité pour tous. En effet, la problématique de la sécurité chez les particuliers est de plus en plus importante. L'environnement informatique des particuliers ne fait que se complexifier en termes de nombre et de diversité d'équipements à gérer (l'ordinateur, la tablette, le smartphone, et tous les objets connectés). L'infrastructure informatique des particuliers n'a plus de frontière physique. En effet, le réseau des particuliers n'est plus limité aux murs de leur habitation. Leurs données sont dans les nuages informatiques, leurs objets connectés sont dans leur voiture, leur poche, etc. L'administration des ces données/objets sera collaborative car partagée entre les membres de la famille, les amis, etc. Par conséquent, je pense que les problématiques que nous avons traitées dans le domaine des organisations virtuelles vont apparaître chez les particuliers. Donc, il est nécessaire de proposer des outils de gestion adaptés aux particuliers à long terme.

Pour l'instant, nous avons travaillé sur la gestion de la confiance dans les certificats X.509 et l'écriture de règles d'autorisation avec un même objectif dans les deux cas : l'utilisateur doit pouvoir prendre une décision de sécurité informée.

Dans un premier temps, nous continuerons donc à améliorer ces éléments. En particulier, il est intéressant de regarder l'évolution de l'initiative de Google qui tente de forcer la généralisation de HTTPS et maintenant pousse la transparence des certificats (Langley et al. 2013; Google 2015). Il y a aussi le projet FIDO (FIDO Alliance 2015) qui regroupe des banques, des systèmes de paiement en ligne ainsi que des acteurs de la sécurité informatique. Ce groupe qui a proposé en Décembre 2014 deux protocoles pour supprimer l'authentification par mot de passe en généralisant l'authentification par clés publiques.

Enfin pour terminer, je désire travailler sur la définition et l'expression d'exigences de sécurité pour le particulier. Notre approche actuelle consiste à apprendre les préférences des utilisateurs. Toutefois, ces préférences étant des données sensibles, elles doivent rester privées. Je pense que nous suivons la bonne voie et qu'il faut continuer à la défricher. Pour l'instant, nous ne considérons pas dans l'apprentissage les exceptions et/ou les changements de comportements de l'utilisateur par rapport à des propositions acceptées. Nous devons aussi mieux informer l'utilisateur par rapport aux risques qu'il encoure à autoriser ou non des accès à ses ressources informatiques.

Références

Abrial, Jean-Raymond, Jean-Raymond Abrial, et A. Hoare. 2005. *The B-book: assigning programs to meanings*. Cambridge University Press. https://books.google.fr/books?hl=fr&lr=&id=T_ShHENlqBAC&oi=fnd&pg=PP1&dq=the+b-book&ots=Pg8rvn9Tkh&sig=hSisrEXRCd0Jp3a7AwhKRGO6xaw.

Adomavicius, Gediminas, et Alexander Tuzhilin. 2005. « Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions ». *Knowledge and Data Engineering, IEEE Transactions on* 17 (6): 734–749.

AGIMO. 2009. « Gatekeeper PKI framework: Cross recognition policy ». Australian Government Information Management Office. http://www.finance.gov.au/files/2012/04/Cross_Recognition_Policy.rtf.

Agrawal, Dakshi, Kang-Won Lee, et Jorge Lobo. 2005. « Policy-based management of networked computing systems ». *Communications Magazine, IEEE* 43 (10): 69–75.

Ajam, Nabil, Nora Cuppens-Boulahia, et Fréderic Cuppens. 2010. « Contextual privacy management in extended role based access control model ». In *Data Privacy Management and Autonomous Spontaneous Security*, 121–135. Springer. http://link.springer.com/chapter/10.1007/978-3-642-11207-2_10.

Alfaro, Joaquin Garcia, Nora Boulahia-Cuppens, et Frédéric Cuppens. 2008. « Complete analysis of configuration rules to guarantee reliable network security policies ». *International Journal of Information Security* 7 (2): 103–122.

Al-Shaer, Ehab, Hazem Hamed, Raouf Boutaba, et Masum Hasan. 2005. « Conflict classification and analysis of distributed firewall policies ». *Selected Areas in Communications, IEEE Journal on* 23 (10): 2069–2084.

Al-Shaer, Ehab, Will Marrero, Adel El-Atawy, et Khalid Elbadawi. 2009. « Network configuration in a box: Towards end-to-end verification of network reachability and security ». In *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*, 123–132. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5339690.

Al-Shaer, Ehab S., et Hazem H. Hamed. 2004. « Discovery of policy anomalies in distributed firewalls ». In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 4:2605–2616. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1354680.

American Bar Association. 2001. « PKI Assessment Guidelines, v0. 30 ». *Public Draft For Comment*.

Arcangeli, Jean-Paul, Raja Boujbel, et Sébastien Leriche. 2015. « Automatic deployment of distributed software systems: Definitions and state of the art ». *Journal of Systems and Software* 103: 198–218.

Ardagna, Claudio Agostino, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Eros Pedrini, et Pierangela Samarati. 2009. « An XACML-based privacy-centered access control system ». In *Proceedings of the first ACM workshop on Information security governance*, 49–58. ACM. http://dl.acm.org/citation.cfm?id=1655178.

Arnbak, Axel, Hadi Asghari, Michel Van Eeten, et Nico Van Eijk. 2014. « Security collapse in the HTTPS market ». *Communications of the ACM* 57 (10): 47–55.

Asia PKI forum. 2005. « Asia PKI Interoperability Guideline ». Asia PKI Forum - Interoperability Working Group. https://www.oasis-open.org/committees/download.php/13084/APKI_IG_ver2_0_Book1.doc.

Baglin, Gérard, et Mario Capraro. 2002. *L'entreprise étendue et le développement des fournisseurs*. https://hal.archives-ouvertes.fr/hal-00655489/.

Bajaj, Siddharth, Giovanni Della-Libera, Brendan Dixon, Mike Dusche, Maryann Hondo, Matt Hur, Chris Kaler, *et autres*. 2003. « Web services federation language (ws-federation) ». *Retrieved April* 14: 2005.

Balana XACML. 2016. « wso2/balana ». *GitHub*. https://github.com/wso2/balana.

Barker, Steve. 2009. « The next 700 access control models or a unifying meta-model? » In *Proceedings of the 14th ACM*

symposium on Access control models and technologies, 187–196. ACM. http://dl.acm.org/citation.cfm?id=1542238.

Barrere, François, Abdelmalek Benzekri, Frédéric Grasset, et Romain Laborde. 2002. « A multi-domain security policy distribution architecture for dynamic IP based VPN management ». In *Policies for Distributed Systems and Networks, 2002. Proceedings. Third International Workshop on*, 224–227. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1011313.

Basile, Cataldo, et Antonio Lioy. 2004. « Towards an algebraic approach to solve policy conflicts ». In . http://www.cse.chalmers.se/~andrei/FCS04/basile.pdf.

Bell, D. Elliott, et Leonard J. LaPadula. 1973. *Secure computer systems: Mathematical foundations*. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=AD0770768.

Bell, D.E. 2005. « Looking back at the Bell-La Padula model ». In *Computer Security Applications Conference, 21st Annual*, 15 pp.-pp.351. doi:10.1109/CSAC.2005.37.

Biba, Kenneth J. 1977. *Integrity considerations for secure computer systems*. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA039324.

Bix, Brian, et Jane K. Winn. 2006. « Diverging Perspectives on Electronic Contracting in the US and the EU ». *Diverging Perspectives on Electronic Contracting in the US and the EU. Cleveland State Law Review* 54: 175–190.

Bloem, Jaap. 2014. « How the 2010-2020 Decade of Smart Became the Multi-trillion Dollar Decade of SMACT - SogetiLabs ». http://labs.sogeti.com/how-the-2010-2020-decade-of-smart-became-the-multi-trillion-dollar-decade-of-smact/.

Bouyssou, D., D. Dubois, M. Pirlot, et H. Prade. 2006. « Concepts et méthodes pour l'aide à la décision, volume 3, analyse multicritère ». *Hermès*.

Boytsov, Andrey, et Arkady Zaslavsky. 2013. « Formal verification of context and situation models in pervasive computing ». *Pervasive and Mobile Computing*, Special Section: Pervasive Sustainability, 9 (1): 98-117. doi:10.1016/j.pmcj.2012.03.001.

Browne, Jim, et Jiangang Zhang. 1999. « Extended and virtual enterprises-similarities and differences ». *International Journal of Agile Management Systems* 1 (1): 30–36.

Buttyán, Levente, Gábor Pék, et T. Thong. 2009. « Consistency verification of stateful firewalls is not harder than the stateless case ». *Infocommunications Journal* 64 (1): 2–8.

Byun, Ji-Won, Elisa Bertino, et Ninghui Li. 2005. « Purpose based access control of complex data for privacy protection ». In *Proceedings of the tenth ACM symposium on Access control models and technologies*, 102–110. ACM. http://dl.acm.org/citation.cfm?id=1063998.

CA/Browser Forum. 2014. « Guidelines For The Issuance And Management Of Extended Validation Certificates ». https://cabforum.org/wp-content/uploads/EV-SSL-Certificate-Guidelines-Version-1.4.6.pdf.

Castelluccia, Claude, Peter Druschel, S. Fischer Hübner, Aljosa Pasic, Bart Preneel, et Hannes Tschofenig. 2011. « Privacy, accountability and Trust-Challenges and opportunities ». *ENISA.[Online]. Available: http://www. enisa. europa. eu/activities/identity-and-trust/library/deliverables/pat-study/at download/fullReport*.

Cauvin, Emmanuel. 2015. « La vie privée sur Internet expliquée par « Secret Story » ». *Rue89 Les Blogs*. http://blogs.rue89.nouvelobs.com/nouveau-monde/2015/09/22/la-vie-privee-sur-internet-expliquee-par-secret-story-234978.

Cervantes, Humberto, et Richard S. Hall. 2004. « Autonomous adaptation to dynamic availability using a service-oriented component model ». In *Proceedings of the 26th International Conference on Software Engineering*, 614–623. IEEE Computer Society. http://dl.acm.org/citation.cfm?id=999465.

Chadwick, David W., et Alexander Otenko. 2003. « The PERMIS X.509 role based privilege management infrastructure ». *Future Generation Computer Systems*, Selected Papers from the TERENA Networking Conference 2002, 19 (2): 277-289. doi:10.1016/S0167-739X(02)00153-X.

Chadwick, David W., Linying Su, et Romain Laborde. 2009. *Use of XACML Request Context to Obtain an Authorisation Decision*. GFD-R-P.159. https://www.ogf.org/documents/GFD.159.pdf.

Chase, Melissa, et Sherman SM Chow. 2009. « Improving privacy and security in multi-authority attribute-based encryption ». In *Proceedings of the 16th ACM conference on Computer and communications security*, 121–130. ACM. http://dl.acm.org/citation.cfm?id=1653678.

Chaum, David L. 1981. « Untraceable electronic mail, return addresses, and digital pseudonyms ». *Communications of the ACM* 24 (2): 84–90.

Cheaito, M., R. Laborde, F. Barrere, et A. Benzekri. 2009. « An extensible XACML authorization decision engine for context aware applications ». In *Pervasive Computing (JCPC), 2009 Joint Conferences on*, 377-382. doi:10.1109/JCPC.2009.5420155.

Cheaito, Marwan. 2012. « Un cadre de spécification et de déploiement de politiques d'autorisation ». Université de Toulouse, Université Toulouse III-Paul Sabatier. http://thesesups.ups-tlse.fr/1617/.

Cheaito, Marwan, Romain Laborde, François Barrère, et Abdelmalek Benzekri. 2010a. « A deployment framework for self-contained policies ». In *Network and Service Management (CNSM), 2010 International Conference on*, 88-95. doi:10.1109/CNSM.2010.5691328.

Cheaito, Marwan, Romain Laborde, François Barrère, et Abdelmalek Benzekri. 2010b. « Configurable Data Types in Policy Based Access Control Management: A Specification and Enforcement Framework ». In *Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2010), Menton-France*, 18:2010–21.

Chung, Lawrence, et Nary Subramanian. 2004. « Adaptable architecture generation for embedded systems ». *Journal of Systems and Software* 71 (3): 271-295. doi:10.1016/S0164-1212(03)00009-8.

Clark, David D., et David R. Wilson. 1987. « A comparison of commercial and military computer security policies ». In *Security and Privacy, 1987 IEEE Symposium on*, 184–184. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6234890.

CLUSIF. 2007. *Gestion des Identités*. CLUSIF. https://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-Gestion-des-identites.pdf.

Costa, Patricia Dockhorn, Giancarlo Guizzardi, Joao Paulo A. Almeida, Luis Ferreira Pires, et Marten van Sinderen. 2006. « Situations in Conceptual Modeling of Context. » In *EDOC Workshops*, 6. http://www.researchgate.net/profile/Luis_Ferreira_Pires/publication/221142456_Situations_in_Conceptual_Modeling_of_Context/links/0deec5191f848c67b8000000.pdf.

Covington, Michael J., et Manoj R. Sastry. 2006. « A contextual attribute-based access control model ». In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, 1996–2006. Springer. http://link.springer.com/chapter/10.1007/11915072_108.

« CPN Tools ». 2015. Consulté le septembre 23. http://cpntools.org/.

Cranor, Lorrie, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, et Joseph Reagle. 2002. « The platform for privacy preferences 1.0 (P3P1. 0) specification ». *W3C recommendation* 16. http://elearn.inf.tu-dresden.de/hades/teleseminare/wise0405/Act.%208%20Models%20Languages%20Pierangela/Materials/P3P.pdf.

Cugola, Gianpaolo, et Alessandro Margara. 2012. « Processing flows of information: From data stream to complex event processing ». *ACM Computing Surveys (CSUR)* 44 (3): 15.

Cuppens, Frédéric, Nora Cuppens-Boulahia, Joaquin Garcia-Alfaro, Tarik Moataz, et Xavier Rimasson. 2012. « Handling stateful firewall anomalies ». In *Information Security and Privacy Research*, 174–186. Springer. http://link.springer.com/chapter/10.1007/978-3-642-30436-1_15.

Cuppens, Frédéric, Nora Cuppens-Boulahia, et Joaquın Garcıa-Alfaro. 2015. « DETECTION AND REMOVAL OF FIREWALL MISCONFIGURATION ». Consulté le septembre 14. http://www.ccd.uab.es/~joaquin/papers/cnis05.pdf.

Cuppens, Frédéric, et Alexandre Miège. 2003. « Modelling contexts in the Or-BAC model ». In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, 416–425. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1254346.

Danezis, George, et Seda Gürses. 2010. « A critical review of 10 years of privacy technology ». *Proceedings of Surveillance Cultures: A Global Surveillance Society*. http://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf.

Danwei, Chen, Huang Xiuli, et Ren Xunyi. 2009. « Access control of cloud service based on ucon ». In *Cloud computing*, 559–564. Springer. http://link.springer.com/chapter/10.1007/978-3-642-10665-1_52.

Deffains, Bruno, et Jane K. Winn. 2008. « Governance of Electronic Commerce in Consumer and Business Markets ». *GOVERNANCE, REGULATIONS AND POWERS ON THE INTERNET, E. Brousseau, M. Marzouki, C. Méadel, eds., Cambridge University Press*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1099516.

Denecker, Marc, et Eugenia Ternovska. 2007. « Inductive situation calculus ». *Artificial Intelligence* 171 (5–6): 332-360. doi:10.1016/j.artint.2007.02.002.

Dey, Anind K. 2001. « Understanding and Using Context ». *Personal Ubiquitous Comput.* 5 (1): 4–7. doi:10.1007/s007790170019.

Dingledine, Roger, Nick Mathewson, et Paul Syverson. 2004. *Tor: The second-generation onion router*. DTIC Document. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA465464.

El Kateb, Donia, Yehia ElRakaiby, Tejeddine Mouelhi, Iram Rubab, et Yves Le Traon. 2014. « Towards a Full Support of Obligations In XACML ». In *Risks and Security of Internet and Systems*, 213–221. Springer. http://link.springer.com/chapter/10.1007/978-3-319-17127-2_14.

El Khoury, Hicham. 2014. « Une modélisation formelle orientée flux de données pour l'analyse de configuration de sécurité réseau ». Université de Toulouse, Université Toulouse III-Paul Sabatier. http://thesesups.ups-tlse.fr/2499/.

El Khoury, Hicham, Romain Laborde, Francois Barrere, Abdelmalek Benzekri, et Maroun Chamoun. 2011. « A generic data flow security model ». In *Configuration Analytics and Automation (SAFECONFIG), 2011 4th Symposium on*, 1–2. IEEE. http://scholar.google.com/scholar?cluster=3221512353957342853&hl=en&oi=scholarr.

El Khoury, Hicham, Romain Laborde, Francois Barrere, Abdelmalek Benzekri, et Maroun Chamoun. 2013. « A specification method for analyzing fine grained network security mechanism configurations ». In *Communications and Network Security (CNS), 2013 IEEE Conference on*, 483–487. IEEE. http://oatao.univ-toulouse.fr/12724/.

El Khoury, Hicham, Romain Laborde, François Barrère, Maroun Chamoun, et Abdelmalek Benzekri. 2012. « A Formal Data Flow-Oriented Model For Distributed Network Security Conflicts Detection ». In *ICNS 2012, The Eighth International Conference on Networking and Services*, 20–27. http://scholar.google.com/scholar?cluster=3402823843212373271&hl=en&oi=scholarr.

El–Khoury, Hicham, Romain Laborde, François Barrère, Abdelmalek Benzekri, et Maroun Chamoun. 2014. « A data flow–oriented specification method for analysing network security configurations ». *International Journal of Internet Protocol Technology* 8 (2): 58–76.

Elrakaiby, Yehia, Frédéric Cuppens, et Nora Cuppens-Boulahia. 2012. « Formal enforcement and management of obligation policies ». *Data & Knowledge Engineering* 71 (1): 127–147.

EsperTech. 2015. « Chapter 5. EPL Reference: Clauses ». http://www.espertech.com/esper/release-5.3.0/esper-reference/html/epl_clauses.html.

ETSI. 2007. « Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates ». http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf.

ETSI. 2011. « Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs ». http://www.etsi.org/deliver/etsi_tr/101500_101599/101564/01.01.01_60/tr_101564v010101p.pdf.

Ferraiolo, David, Janet Cugini, et D. Richard Kuhn. 1995. « Role-based access control (RBAC): Features and motivations ». In *Proceedings of 11th annual computer security application conference*, 241–48. http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-cugini-kuhn-95.pdf.

Ferraiolo, David, D. Richard Kuhn, et Ramaswamy Chandramouli. 2003. *Role-based access control*. Artech House. https://books.google.fr/books?hl=fr&lr=&id=48AeIhQLWckC&oi=fnd&pg=PR15&dq=Role-Based+Access+Control&ots=LLUEIGxWJ9&sig=DGdginVY9AsFIejUor7B5TWmA3w.

FIDO Alliance. 2015. « FIDO Alliance » Specifications Overview ». https://fidoalliance.org/specifications/overview/.

FPKIPA. 2012. « Criteria and Methodology For Cross-certification with the U.S. Federal Bridge Certification Authority (FBCA) ». http://idmanagement.gov/sites/default/files/documents/crosscert_method_criteria%20v3.0%20%282%29_0.doc.

Friedman, Arik, Bart P. Knijnenburg, Kris Vanhecke, Luc Martens, et Shlomo Berkovsky. 2015. « Privacy aspects of recommender systems ». In *Recommender Systems Handbook*, 649–688. Springer. http://link.springer.com/chapter/10.1007/978-1-4899-7637-6_19.

Fu, Zhi, S. Felix Wu, He Huang, Kung Loh, Fengmin Gong, Ilia Baldine, et Chong Xu. 2001. « IPSec/VPN security policy: Correctness, conflict detection, and resolution ». In *Policies for Distributed Systems and Networks*, 39–56. Springer. http://link.springer.com/chapter/10.1007/3-540-44569-2_3.

Gama, João, Indrė Žliobaitė, Albert Bifet, Mykola Pechenizkiy, et Abdelhamid Bouchachia. 2014. « A survey on concept drift adaptation ». *ACM Computing Surveys (CSUR)* 46 (4): 44.

Garcia-Alfaro, Joaquin, Frédéric Cuppens, Nora Cuppens-Boulahia, et Stere Preda. 2011. « MIRAGE: a management tool for the analysis and deployment of network security policies ». In *Data Privacy Management and Autonomous Spontaneous Security*, 203–215. Springer. http://link.springer.com/chapter/10.1007/978-3-642-19348-4_15.

Gentry, Craig. 2009. « Fully homomorphic encryption using ideal lattices. » In *STOC*, 9:169–178. https://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf.

Giard, Vincent Editeur, et Bernard Roy. 1985. *Méthodologie multicritère d'aide à la décision*. Editions Economica. http://documents.irevues.inist.fr/handle/2042/29606.

Giorgini, Paolo, John Mylopoulos, et Roberto Sebastiani. 2005. « Goal-oriented requirements analysis and reasoning in the tropos methodology ». *Engineering Applications of Artificial Intelligence* 18 (2): 159–171.

Google. 2015. « Certificate Transparency ». http://www.certificate-transparency.org/.

Gorry, George Anthony, et Michael S. Scott Morton. 1971. *A framework for management information systems*. Vol. 13. Massachusetts Institute of Technology. http://cpe.njit.edu/dlnotes/MIS645/Frame_Management_Info.pdf.

Gouda, Mohamed G., et Alex X. Liu. 2005. « A model of stateful firewalls and its properties ». In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*, 128–137. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1467787.

Grabisch, Michel, Ivan Kojadinovic, Site Polytech Nantes, et Patrick Meyer. 2006. « Using the Kappalab R package for capacity identification in Choquet integral based MAUT ». In *Proceedings of the 11th international conference on information processing and management of uncertainty in knowledge-based systems*, 1702–1709. Citeseer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.905&rep=rep1&type=pdf.

Grabisch, Michel, et Marc Roubens. 2000. « Application of the Choquet integral in multicriteria decision making ». *Fuzzy Measures and Integrals-Theory and Applications*, 348–374.

Graf, Cornelia, Christina Hochleitner, Peter Wolkerstorfer, Julio Angulo, Simone Fischer-Hübner, Erik Wästlund, Marit Hansen, et Leif-Erik Holtz. 2013. « Towards usable privacy enhancing technologies: lessons learned from the PrimeLife project ». *PrimeLife Deliverable D* 4.

Guttman, Joshua D., et Amy L. Herzog. 2005. « Rigorous automated network security management ». *International Journal of Information Security* 4 (1-2): 29–48.

Hall, Richard, Karl Pauls, Stuart McCulloch, et David Savage. 2011. *OSGi in action: Creating modular applications in Java*.

Manning Publications Co. http://dl.acm.org/citation.cfm?id=2018636.

Hamed, Hazem, et Ehab Al-Shaer. 2006. « Taxonomy of conflicts in network security policies ». *Communications Magazine, IEEE* 44 (3): 134–141.

Hanna, Stephen R., et Jean Pawluk. 2004. « Identifying and overcoming obstacles to pki deployment and usage ». In *3rd Annual PKI R$\backslash$ &D Workshop. NIST, Gaithersburg*. Citeseer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.177.1873&rep=rep1&type=pdf.

Harkins, Malcolm. 2012. *Managing Risk and Information Security: Protect to Enable*. Apress. https://books.google.fr/books?hl=fr&lr=&id=YWdrcDqvjdwC&oi=fnd&pg=PP3&dq=Managing+Risk+and+Information+Security+:+Protect+to+Enable&ots=GuxvbhZY4-&sig=OMHplq3K37UglIDFvq4MYNqMW2k.

Harrison, Michael A., Walter L. Ruzzo, et Jeffrey D. Ullman. 1976. « Protection in operating systems ». *Communications of the ACM* 19 (8): 461–471.

Harry, Guillaume. 2013. *IAM : Gestion des identités et des accès*. https://aresu.dsi.cnrs.fr/IMG/pdf/IAM_gestion_des_identites_et_des_acces.pdf.

Hatebur, Denis, Maritta Heisel, et Holger Schmidt. 2006. « Security engineering using problem frames ». In *Emerging Trends in Information and Communication Security*, 238–253. Springer. http://link.springer.com/chapter/10.1007/11766155_17.

Henning, Rhonda R. 2014. « Security Policies That Make Sense for Complex Systems: Comprehensible Formalism for the System Consumer ». http://nsuworks.nova.edu/gscis_etd/9/.

« HERAS-AF Homepage ». 2015. Consulté le août 31. http://www.herasaf.org/.

Housley, Russell, Warwick Ford, W. Polk, et David Solo. 2008. *Rfc 5280: Internet X. 509 Public Key Infrastructure Certificate and CRL profile*. May.

Huang, Yan, David Evans, Jonathan Katz, et Lior Malka. 2011. « Faster Secure Two-Party Computation Using Garbled Circuits. » In *USENIX Security Symposium*. Vol. 201. https://www.usenix.org/event/sec11/tech/full_papers/Huang.pdf.

Inglesant, Philip, M. Angela Sasse, David Chadwick, et Lei Lei Shi. 2008. « Expressions of expertness: the virtuous circle of natural language for access control policy specification ». In *Proceedings of the 4th symposium on Usable privacy and security*, 77–88. ACM. http://dl.acm.org/citation.cfm?id=1408675.

Interpol. 2015. « Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL ». http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

ISO 7498-2. 1989. « Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture ».

ISO 24760. 2011. *ISO/IEC 24760-1:2011 - Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts*. ISO/IEC 24760-1. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57914.

Jeckmans, Arjan JP, Michael Beye, Zekeriya Erkin, Pieter Hartel, Reginald L. Lagendijk, et Qiang Tang. 2013. « Privacy in recommender systems ». In *Social media retrieval*, 263–281. Springer. http://link.springer.com/chapter/10.1007/978-1-4471-4555-4_12.

Jensen, Kurt. 1987. *Coloured petri nets*. Springer. http://link.springer.com/chapter/10.1007/BFb0046842.

Jiang, Xiaodong, James Landay, et others. 2002. « Modeling privacy control in context-aware systems ». *Pervasive Computing, IEEE* 1 (3): 59–63.

Jones, Anita K., Richard J. Lipton, et Lawrence Snyder. 1976. « A linear time algorithm for deciding security ». In *Foundations of Computer Science, 1976., 17th Annual Symposium on*, 33–41. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4567885.

Jøsang, Audun, John Fabre, Brian Hay, James Dalziel, et Simon Pope. 2005. « Trust requirements in identity management ». In *Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44*, 99–108.

Australian Computer Society, Inc. http://dl.acm.org/citation.cfm?id=1082305.

Joshi, James BD, Elisa Bertino, Usman Latif, et Arif Ghafoor. 2005. « A generalized temporal role-based access control model ». *Knowledge and Data Engineering, IEEE Transactions on* 17 (1): 4–23.

Jung, Taeho, Xiang-Yang Li, Zhiguo Wan, et Meng Wan. 2015. « Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption ». *Information Forensics and Security, IEEE Transactions on* 10 (1): 190–199.

Kabbani, Bashar. 2015. « Unified And Dynamic Policy-Based Framework For Security Management Systems ». Université de Toulouse, Université Toulouse III-Paul Sabatier.

Kabbani, Bashar, Romain Laborde, François Barrere, et Abdelmalek Benzekri. 2014. « Specification and enforcement of dynamic authorization policies oriented by situations ». In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on*, 1–6. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6814050.

Kabbani, Bashar, Romain Laborde, François Barrère, et Abdelmalek Benzekri. 2014. « Managing Break-The-Glass using Situation-oriented authorizations ». In *9ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information-SAR-SSI 2014*, 0. https://hal.archives-ouvertes.fr/hal-01120112/.

Kalam, Anas Abou El, R. E. Baida, Philippe Balbiani, Salem Benferhat, Frédéric Cuppens, Yves Deswarte, Alexandre Miege, Claire Saurel, et Gilles Trouessin. 2003. « Organization based access control ». In *Policies for Distributed Systems and Networks, 2003. Proceedings. POLICY 2003. IEEE 4th International Workshop on*, 120–131. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1206966.

Kamel, M., R. Laborde, F. Barrere, et A. Benzekri. 2009. « SecMaLET: a tool for establishing the chain of trust within a Virtual Enterprise ». In *International Conference on Network and Service Security, 2009. N2S '09*, 1-5.

Kamel, Michel. 2008. « Patrons organisationnels et techniques pour la sécurisation des Organisations virtuelles ». Université de Toulouse, Université Toulouse III-Paul Sabatier. http://thesesups.ups-tlse.fr/326/.

Kamel, Michel, Romain Laborde, François Barrère, et Abdelmalek Benzekri. 2008. « A trust-based virtual collaborative environment. » http://www.dirf.org/jdim/v6n506.pdf.

Karjoth, Günter, Matthias Schunter, et Michael Waidner. 2003. « Platform for enterprise privacy practices: Privacy-enabled management of customer data ». In *Privacy Enhancing Technologies*, 69–84. Springer. http://link.springer.com/chapter/10.1007/3-540-36467-6_6.

Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, et Lorrie Faith Cranor. 2010. « Standardizing privacy notices: an online study of the nutrition label approach ». In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, 1573–1582. ACM. http://dl.acm.org/citation.cfm?id=1753561.

Kennedy, Scott. 2006. « The political economy of standards coalitions: Explaining China's involvement in high-tech standards wars ». *asia policy* 2 (1): 41–62.

Kent, Stephen. 2005. « IP encapsulating security payload (ESP) ». IETF. http://tools.ietf.org/html/rfc4303?ref=driverlayer.com/web.

Laborde, R., M. Cheaito, F. Barrere, et A. Benzekri. 2009. « An Extensible XACML Authorization Web Service: Application to Dynamic Web Sites Access Control ». In *Signal-Image Technology & Internet-Based Systems (SITIS), 2009 Fifth International Conference on*, 499-505. doi:10.1109/SITIS.2009.83.

Laborde, R., M. Kamel, S. Wazan, et F. Barrere. 2009. « A secure collaborative web-based environment for virtual organisations ». *International Journal of Web Based Communities* 5 (2): 273–292.

Laborde, Romain, François Barrère, et Abdelmalek Benzekri. 2013. « Toward authorization as a service: a study of the XACML standard ». In *Proceedings of the 16th Communications & Networking Symposium*, 9. Society for Computer Simulation International. http://dl.acm.org/citation.cfm?id=2499995.

Laborde, Romain, Marwan Cheaito, François Barrère, et Abdelmalek Benzekri. 2010. « Toward self-contained authorization policies ». In *Policies for Distributed Systems and Networks (POLICY), 2010 IEEE International Symposium on*,

103–106. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5630212.

Laborde, Romain, Bashar Kabbani, Francois Barrere, et Abdelmalek Benzekri. 2014. « An adaptive xacmlv3 policy enforcement point ». In *Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International*, 620–625. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6903200.

Laborde, Romain, Michel Kamel, François Barrère, et Abdelmalek Benzekri. 2007. « Implementation of a Formal Security Policy Refinement Process in WBEM Architecture ». *Journal of Network and Systems Management* 15 (2): 241-266. doi:10.1007/s10922-007-9063-z.

Laborde, Romain, Michel Kamel, Fran?ois Barrere, et Abdelmalek Benzekri. 2008. « PEP = Point to Enhance Particularly ». In *Policies for Distributed Systems and Networks, IEEE International Workshop on*, 0:93-96. Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/POLICY.2008.13.

Laborde, Romain, Bassem Nasser, Frédéric Grasset, François Barrère, et Abdelmalek Benzekri. 2005. « A formal approach for the evaluation of network security mechanisms based on RBAC policies ». *Electronic Notes in Theoretical Computer Science* 121: 117–142.

Lampson, Butler W. 1974. « Protection ». *ACM SIGOPS Operating Systems Review* 8 (1): 18–24.

Landau, Susan, et Tyler Moore. 2012. « Economic tussles in federated identity management ». *First Monday* 17 (10). http://128.248.156.56/ojs/index.php/fm/article/view/4254.

Langheinrich, Marc. 2009. *Privacy in ubiquitous computing*. Krumm J (ed). https://vs.inf.ethz.ch/events/dag2001/slides/marc.pdf.

Langley, Adam, Emilia Kasper, et Ben Laurie. 2013. « RFC 6962 - Certificate Transparency ». http://tools.ietf.org/html/rfc6962.

Laufer, Robert S., et Maxine Wolfe. 1977. « Privacy as a concept and a social issue: A multidimensional developmental theory ». *Journal of social Issues* 33 (3): 22–42.

Lounis, Ahmed, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, et Yacine Challal. 2016. « Healing on the cloud: Secure cloud architecture for medical wireless sensor networks ». *Future Generation Computer Systems* 55 (février): 266-277. doi:10.1016/j.future.2015.01.009.

Lymberopoulos, Leonidas, Emil Lupu, et Morris Sloman. 2003. « An adaptive policy-based framework for network services management ». *Journal of Network and systems Management* 11 (3): 277–303.

Machanavajjhala, Ashwin, Daniel Kifer, Johannes Gehrke, et Muthuramakrishnan Venkitasubramaniam. 2007. « l-diversity: Privacy beyond k-anonymity ». *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1 (1): 3.

Mariotti, Fabien, Thomas Reverdy, et Denis Segrestin. 2001. « Du gouvernement d'entreprise au gouvernement de réseau ». *Rapport pour le commissariat Général du Plan, Avril*. http://thomas.reverdy.free.fr/CGPMariotti.pdf.

Marx, Gary T. 2001. « Murky conceptual waters: The public and the private ». *Ethics and Information technology* 3 (3): 157–169.

Matheus, Andreas, et J. Herrmann. 2008. « Geospatial extensible access control markup language (geoxacml) ». *Open Geospatial Consortium Inc. OGC*. http://www.w3.org/Policy/pling/wiki/images/5/59/GeoXACML.pdf.

Meissonier, Régis. 2000. *Vers une perspective processuelle du concept d'organisation virtuelle*. http://cat.inist.fr/?aModele=afficheN&cpsidt=103977.

Mont, Marco Casassa, et Robert Thyne. 2006. « A systemic approach to automate privacy policy enforcement in enterprises ». In *Privacy Enhancing Technologies*, 118–134. Springer. http://link.springer.com/chapter/10.1007/11957454_7.

Morgan, R. L., Scott Cantor, Steven Carmody, Walter Hoehn, et Ken Klingenstein. 2004. « Federated Security: The Shibboleth Approach. » *Educause Quarterly* 27 (4): 12–17.

Moringiello, Juliet M., et William L. Reynolds. 2008. « Survey of the Law of Cyberspace: Electronic Contracting Cases 2007-2008 ». *Business Lawyer* 64 (1): 199.

Nasser, Bassem, Romain Laborde, Abdelmalek Benzekri, François Barrère, et Michel Kamel. 2005. « Access control model for inter-organizational grid virtual organizations ». In *On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops*, 537–551. Springer. http://link.springer.com/chapter/10.1007/11575863_73.

Neisse, Ricardo, Alexander Pretschner, et Valentina Di Giacomo. 2011. « A trustworthy usage control enforcement framework ». In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, 230–235. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6045968.

Nergaard, Henrik, Nils Ulltveit-Moe, et Terje Gjøs\a eter. 2015. « A Scratch-based Graphical Policy Editor for XACML ». In *ICISSP 2015 Proceedings of the 1st International Conference on Information Systems Security and Privacy ESEO, Angers, Loire Valley, France*, 182–191. http://semiah.eu/wp-content/uploads/2015/01/A-Scratch-based-Graphical-Policy-Editor-for-XACML.pdf.

NIST ABAC. 2015. « Attribute Based Access Control (ABAC) Overview ». Consulté le août 28. http://csrc.nist.gov/projects/abac/.

OASIS SAML. 2015. « OASIS Security Services (SAML) TC | OASIS ». *SAML*. Consulté le août 28. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

OASIS XACML. 2015. « OASIS eXtensible Access Control Markup Language (XACML) TC | OASIS ». Consulté le août 28. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

OASIS XACMLv3. 2013. *eXtensible Access Control Markup Language (XACML) Version 3.0*. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.pdf.

Oglaza, Arnaud. 2014. « Système d'aide à la décision pour la protection des données de vie privée ». Toulouse 1. http://www.theses.fr/2014TOU10015.

Oglaza, Arnaud, Pascale Zaraté, et Romain Laborde. 2014. « Kapuer: A Decision Support System for Protecting Privacy ». In *Group Decision and Negotiation. A Process-Oriented View*, 100–107. Springer International Publishing. http://link.springer.com/chapter/10.1007/978-3-319-07179-4_11.

OpenGroup. 2014. « The Nexus of Forces in Action ». http://www.opengroup.org/openplatform3.0/docs/Use-Cases/title.htm.

« OSGi Alliance ». 2015. Consulté le septembre 1. http://www.osgi.org/Main/HomePage.

Papazoglou, Michael P., Paolo Traverso, Schahram Dustdar, et Frank Leymann. 2007. « Service-oriented computing: State of the art and research challenges ». *Computer*, n° 11: 38–45.

Park, Jaehong, et Ravi Sandhu. 2004. « The UCON ABC usage control model ». *ACM Transactions on Information and System Security (TISSEC)* 7 (1): 128–174.

Park, Seon-Ho, Young-Ju Han, et Tai-Myoung Chung. 2006. « Context-role based access control for context-aware application ». In *High Performance Computing and Communications*, 572–580. Springer. http://link.springer.com/chapter/10.1007/11847366_59.

Petrie, Charles, et Volker Roth. 2015. « How Badly Do You Want Privacy? » *IEEE Internet Computing*, n° 2: 92–94.

Pfitzmann, Andreas, et Michael Waidner. 1986. « Networks without user observability—design options ». In *Advances in Cryptology—EUROCRYPT'85*, 245–253. Springer. http://link.springer.com/chapter/10.1007/3-540-39805-8_29.

Polk, William T., et Nelson E. Hastings. 2000. « Bridge certification authorities: Connecting b2b public key infrastructures ». In *PKI Forum Meeting Proceedings*, 27–29. http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/B2B-article.pdf.

Preda, Stere, Nora Cuppens-Boulahia, Frédéric Cuppens, Joaquin Garcia-Alfaro, et Laurent Toutain. 2010. « Model-driven security policy deployment: Property oriented approach ». In *Engineering secure software and systems*, 123–139. Springer. http://link.springer.com/chapter/10.1007/978-3-642-11747-3_10.

Rass, Stefan. 2013. « Blind Turing-Machines: Arbitrary Private Computations from Group Homomorphic Encryption ». *International Journal of Advanced Computer Science and Applications* 4 (11): 47-56.

Regev, Gil, et Alain Wegmann. 2005. « Where do goals come from: the underlying principles of goal-oriented requirements engineering ». In *Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on*, 353–362.

IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1531055.

Ross, Ron, Janet Carrier Oren, et Michael McEvilley. 2014. « System Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems. National Institute of Standards and Technology ». *NIST Special publication*, 800–160.

« RuleML Wiki ». 2015. Consulté le septembre 2. http://wiki.ruleml.org/index.php/RuleML_Home.

Sahai, Amit, et Brent Waters. 2005. « Fuzzy identity-based encryption ». In *Advances in Cryptology–EUROCRYPT 2005*, 457–473. Springer. http://link.springer.com/chapter/10.1007/11426639_27.

Saltzer, J.H., et M.D. Schroeder. 1975. « The protection of information in computer systems ». *Proceedings of the IEEE* 63 (9): 1278-1308. doi:10.1109/PROC.1975.9939.

Samarati, Pierangela, et Sabrina de Vimercati. 2001. « Access Control: Policies, Models, and Mechanisms ». *Foundations of Security Analysis and Design*, 137–196.

Sandhu, Ravinderpal Singh. 1988. « The schematic protection model: its definition and analysis for acyclic attenuating schemes ». *Journal of the ACM (JACM)* 35 (2): 404–432.

Shi, Leilei, et David W. Chadwick. 2011. « A Controlled Natural Language Interface for Authoring Access Control Policies ». In *Proceedings of the 2011 ACM Symposium on Applied Computing*, 1524–1530. SAC '11. New York, NY, USA: ACM. doi:10.1145/1982185.1982510.

Simon, Herbert A. 1972. « Theories of bounded rationality ». *Decision and organization* 1 (1): 161–176.

Sloman, Morris, et Emil Lupu. 2002. « Security and management policy specification ». *Network, IEEE* 16 (2): 10–19.

Smith, H. Jeff, Tamara Dinev, et Heng Xu. 2011. « Information privacy research: an interdisciplinary review ». *MIS quarterly* 35 (4): 989–1016.

Smith, P. 2000. « Trust and Digital Certificates ». In *16th Payment Systems International Conference*.

Solove, Daniel J. 2006. « A taxonomy of privacy ». *University of Pennsylvania law review*, 477–564.

Stepien, Bernard, Amy Felty, et Stan Matwin. 2014. « A non-technical XACML target editor for dynamic access control systems ». In *Collaboration Technologies and Systems (CTS), 2014 International Conference on*, 150–157. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6867558.

Sun XACML. 2016. « Sun's XACML Implementation Programmer's Guide ». http://sunxacml.sourceforge.net/guide.html.

Sweeney, Latanya. 2002. « k-anonymity: A model for protecting privacy ». *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (5): 557–570.

Thomas, Roshan K. 1997. « Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments ». In *Proceedings of the second ACM workshop on Role-based access control*, 13–19. ACM. http://dl.acm.org/citation.cfm?id=266748.

Tsai, Wei-Tek, Zhibin Cao, Xiao Wei, Ray Paul, Qian Huang, et Xin Sun. 2007. « Modeling and simulation in service-oriented software development ». *Simulation* 83 (1): 7–32.

UNCITRAL. 2009. *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*.

Uribe, Tomás E., et Steven Cheung. 2004. « Automatic analysis of firewall and network intrusion detection system configurations ». In *Proceedings of the 2004 ACM workshop on Formal methods in security engineering*, 66–74. ACM. http://dl.acm.org/citation.cfm?id=1029143.

Uzunov, Anton V., Eduardo B. Fernandez, et Katrina Falkner. 2012. « Engineering Security into Distributed Systems: A Survey of Methodologies. » *J. UCS* 18 (20): 2920–3006.

Van Lamsweerde, Axel. 2009. « Requirements engineering: from system goals to UML models to software specifications ».

Vollbrecht, J., P. Calhoun, Stephen Farrell, Leon Gommans, G. Gross, Betty de Bruijn, Cees de Laat, Matt Holdrege, et D. Spence. 2000. « RFC 2904: AAA Authorization Framework ». *Request For Comment, Network Working Group*.

W3 Schools. 2015. « XML Tutorial ». Consulté le septembre 14. http://www.w3schools.com/xml/.

Wagealla, Waleed, Sotirios Terzis, et Colin English. 2003. « Trust-based model for privacy control in context aware

systems ». In *Second workshop on security in ubiquitous computing at the fifth annual conference on ubiquitous computing (UbiComp2003)*. http://strathprints.strath.ac.uk/2521/.

Warren, Samuel D., et Louis D. Brandeis. 1890. « The right to privacy ». *Harvard law review*, 193–220.

Watson, Paul. 2012. « A Multi-Level Security Model for Partitioning Workflows over Federated Clouds ». *Journal of Cloud Computing* 1 (1): 1-15. doi:10.1186/2192-113X-1-15.

Wazan, Ahmad, Romain Laborde, David Chadwick, François Barrere, et AbdelMalek Benzekri. 2009. « Which Web Browsers Process SSL Certificates in a Standardized Way? » *Emerging Challenges for Security, Privacy and Trust*, 432–442.

Wazan, Ahmad Samer. 2011. « Gestion de la confiance dans les infrastructures à clés publiques ». Toulouse 3. http://www.theses.fr/2011TOU30233.

Wazan, Ahmad Samer, Romain Laborde, Francois Barrere, et Abdelmalek Benzekri. 2011. « A formal model of trust for calculating the quality of X. 509 certificate ». *Security and Communication Networks* 4 (6): 651–665.

Wazan, Ahmad Samer, Romain Laborde, François Barrere, Abdelmalek Benzekri, et David W. Chadwick. 2013. « PKI Interoperability: Still an Issue? A Solution in the X. 509 Realm ». In *Information Assurance and Security Education and Training*, 68–82. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-39377-8_8.

Winn, Jane. 2006. « Information Technology Standards as a Form of Consumer Protection Law ». *Consumer Protection in the Age of the 'Information Economy,'Ashgate*. http://www.law.washington.edu/directory/docs/winn/info_tech_stds.pdf.

Winn, Jane, et Nicolas Jondet. 2008. « A "New Approach" to standards and consumer protection ». *Journal of consumer policy* 31 (4): 459–472.

Winn, Jane K. 2009. « What Protection Do Consumers Require in the Information Economy? » *Ethics, Law, and Society* 4: 303.

XMLENC, XML. 2002. *Encryption Syntax and Processing, W3C Recommendation 10 December 2002*.

Ye, Juan, Simon Dobson, et Susan McKeever. 2012. « Situation identification techniques in pervasive computing: A review ». *Pervasive and Mobile Computing* 8 (1): 36-66. doi:10.1016/j.pmcj.2011.01.004.

Ylitalo, Jukka, et Pekka Nikander. 2006. « BLIND: A complete identity protection framework for end-points ». In *Security Protocols*, 163–176. Springer. http://link.springer.com/chapter/10.1007/11861386_18.

Zhang, Hong, Yeping He, et Zhiguo Shi. 2006. « Spatial context in role-based access control ». In *Information Security and Cryptology–ICISC 2006*, 166–178. Springer. http://link.springer.com/chapter/10.1007/11927587_15.

Annexe : Curriculum Vitae

Nom : LABORDE **Prénom :** Romain
Né(e) le : 18/10/1978

I – PARCOURS UNIVERSITAIRE

2001 - 2005
Doctorat, Groupe SIERA, IRIT, Université Paul Sabatier, Toulouse, France. *Mémoire*: "Un cadre formel pour le raffinement de l'information de gestion de la sécurité réseau : Expression et Analyse".

2000 - 2001
DEA Réseau & Télécom, Université Paul Sabatier, Toulouse, France. *Mémoire*: "Distribution de politiques IPsec".

1999 - 2000
Maîtrise Informatique, Université de Pau et des Pays de l'Adour, Pau, France.

1998 - 1999
Licence Informatique, Université de Pau et des Pays de l'Adour, Pau, France.

1996 - 1998
DEUG MIAS, Université de Pau et des Pays de l'Adour, Pau, France.

II – PARCOURS PROFESSIONNEL

depuis 2006
Maître de conférences en informatique, Groupe SIERA, IRIT, IUT A - Université Paul Sabatier, Toulouse, France.

2005 - 2006
Research Associate, Groupe ISSR, Computing Laboratory, University of Kent at Canterbury, United Kingdom.

2004 - 2005
ATER (mi temps), Université Paul Sabatier, Toulouse, France.

2001 - 2004
Moniteur, Université Paul Sabatier, Toulouse, France.

III – ACTIVITES D'ENSEIGNEMENT (depuis 2006)

IUT (formation initiale) (depuis 2006)
L1 : Réseau, Système d'exploitation, Architecture/Assembleur, Programmation C, Administration réseau/système, Informatique et Ethique
L2 : Programmation système, Programmation réseau

IUT (Année Spéciale) (depuis 2007)
L1/L2 : Réseau, Programmation réseau, Administration réseau

Master 1 STRI et 2ème année spécialité TRI UPSITECH (depuis 2006)
Sécurité réseau

Master 2 ASIC (depuis 2009)
Sécurité dans les organisations virtuelles

DU 3SI (niveau M2) (depuis 2014)
Sécurité réseau, Gestion des accès et des identités

Licence Pro SIL Sécurité des Systèmes et des Réseaux (2006 -> 2010)
Techniques de gestion liées à la sécurité

Master 2 CAMSI (2007 et 2008)
Sécurité dans les systèmes répartis

IV – ACTIVITES D'ENCADREMENT

Co-Encadrement d'étudiants en Doctorat (Thèses en cours)

- Ibrahim Yonis Omar (depuis Septembre 2012), "Gestion de la sécurité dans les environnements d'e-gouvernement" (co-encadrement avec F. Barrère et A. Benzekri).
- Sravani Teja Bulusu (depuis Septembre 2015 -> ??), "Ingénierie des exigences de sécurité et de supervision réseau" (co-encadrement avec F. Barrère, A. Benzekri, et A. S. Wazan).

Co-Encadrement d'étudiants en Doctorat (Thèses soutenues)

- Bashar Kabbani (Septembre 2011 -> 29 Octobre 2015), "Gestion unifiée et dynamique de la sécurité: Un cadriciel dirigé par les situations" (co-encadrement avec F. Barrère et A. Benzekri). Implication dans l'encadrement 50%.
- Arnaud Oglaza (Septembre 2011 -> 12 Septembre 2014), "Système d'aide à la décision pour la protection des données de vie privée" (co-encadrement avec P. Zaraté). Implication dans l'encadrement 50%.
- Hicham El Khouri (Septembre 2008 ->15 Septembre 2014), "Une modélisation formelle orientée flux de données pour l'analyse de configuration de sécurité réseau" (co-encadrement avec F. Barrère et A. Benzekri). Implication dans l'encadrement 50%.
- Marwan Cheaito (Septembre 2007 - 9 Mars 2012), "Un cadre de spécification et de déploiement de politiques d'autorisation" (co-encadrement avec F. Barrère et A. Benzekri). Implication dans l'encadrement 50%.
- Samer Wazan (Septembre 2007 - 9 Décembre 2011), "Gestion de la confiance dans les infrastructures à clés publiques" (co-encadrement avec F. Barrère et A. Benzekri). Implication dans l'encadrement 50%.
- Michel Kamel (Janvier 2005 – décembre 2008), "Patrons organisationnels et techniques pour la sécurisation des Organisations virtuelles" (co-encadrement avec F. Barrère et A. Benzekri). Implication dans l'encadrement 10%.

Co-Encadrement d'étudiants niveau Master2/DEA

- Serene Najdi (2009), "Implementing a modular architecture for the Policy Enforcement Point".
- Hicham El Khouri (2007), "Développement d'un agent de gestion CIM object Provider dans l'architecture WBEM".
- Samer Wazan (2007), "Une Etude des modèles de réputation dans le contexte des infrastructures de gestion de clés".
- Michel Kamel (2004), "Contribution à la gestion de la sécurité réseau : dérivation de modèles".
- Patrick Trabé (2003), "Sécurisation de flux de données à caractères dynamiques".

VI - AUTRES

Travaux liés à la standardisation

Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri, D.W. Chadwick. Proposition summary to X.509 committee: Adding the role of technical and juridical expert to the X.509 trust model - ITU Study group 17 - TD 0131. avril 2013.

D.W. Chadwick, L. Su, Romain Laborde. Use of XACML Request Context to Obtain an Authorisation Decision. Diffusion scientifique. novembre 2009. Open Grid Forum, OGSA Authorization WG, GFD Proposed Recommendation, P-REC 159

Collaborations dans des projets

Projets en cours

- 2014-2018 : projet DGA/DGAC IREHDO2 (Intégration REseau Haut Débit embarqué Optique 2ème phase) (référent de l'équipe SIERA pour les échanges/comités techniques avec le responsable du projet IREHDO2)
- 2014 – 2017 : projet FUI BOX@PME

Projets terminés :

- 2012 – 2015 : projet ANR INCOME (INfrastructure de gestion de COntexte Multi-Echelle pour l'Internet des Objets)
- 2011-2014 : projet européen ITEA2 PREDYKOT (Policies REfined DYnamically and Kept On Track)
- 2009 – 2012 : projet IMAP (Information Management for Avionics Platform) - DGAC
- 2008 – 2011 : projet FUI GeoWINE
- 2006 : Projet coopération AIRSYS IFAU - Ip For Avionic Uses
- 2004 – 2008 : Projet européen VIVACE - Value Improvement Through a Virtual Aeronautical Collaborative Enterprise

Participation à la vie de l'Université

- Co-responsable de la gestion des stages au département informatique IUT'A' (depuis 2014)
- Membre élu du conseil scientifique de l'Université Paul Sabatier (2010 -> 2012)
- Membre du comité de pilotage de l'appel d'offre du conseil scientifique de l'UPS : opérations scientifiques 2011-2012 (Juillet 2010 – février 2011)

Animations scientifiques

Membre du comité d'organisation de:

- 10th International Conference on Availability, Reliability and Security (ARES 2015)
- 1st International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and New Technologies (SVM 2007)
- 6ème colloque francophone sur Gestion de REseaux et de Services (GRES 2005)

Membre du comité de rédaction de:

- International Journal on Advances in Telecommunications (2012 ->)
- Advances in E-Business Research Book Series (2009 -> 2013)

Co-Président de programme de :

- Special track on Trust and Security - International Conference on Pervasive Computing and Applications 2009 (Avec G. Zhao de South China Normal University)

Membre du comité de programme de :

- IEEE International Conference on Advanced and Trusted Computing (ATC)
  2016
- Workshop on Middleware for Context-Aware Applications in the IoT (M4IOT)
  2014, 2015
- International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING)
  2013, 2014, 2015

- International Conference on Systems and Networks Communications (ICSNC)
  2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016
- IFIP Conference on Communications and Multimedia Security (CMS)
  2012, 2013, 2014
- International Conference on Information Assurance and Security (IAS)
  2007, 2008, 2009; 2010, 2011, 2012, 2013, 2014
- International Conference on Human-Centered Computing (HCC)
  2014
- International Conference on Pervasive Computing and Applications (ICPCA)
  2011, 2012, 2013
- Workshop on Cloud and Super Computing (CSC)
  2013
- Summer FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-Summer)
  2012
- IEEE International Conference on Cloud Computing Technology and Science (CloudCom)
  2009, 2010, 2011
- International Symposium on Security and Multimodality in Pervasive Environments (SMPE)
  2008, 2009, 2010, 2011
- International Workshop on Trustworthiness, Reliability and services in Ubiquitous and Sensor neTworks (TRUST)
  2006, 2007
- International Workshop on Service, Security and its Data management for Ubiquitous Computing (SSDU)
  2007

Liste complète des publications

Articles de revues internationales / International journal papers

- Arnaud Oglaza, Pascale Zaraté, Romain Laborde. *KAPUER: A Decision Support System for Privacy Policies Specification.* Dans : *Annals of Data Science*, Springer-Verlag, Vol. 2 N. 1, p. 1-23, février 2015. Accès : DOI 10.1007/s40745-014-0027-3
- Hicham El Khoury, Romain Laborde, François Barrère, Maroun Chamoun, Abdelmalek Benzekri. *A Data Flow Oriented Specification Method for Analyzing Network Security Configurations.* Dans : *International Journal of Internet Protocol Technology*, Inderscience Publishers, Numéro spécial *Innovative Mobile and Internet Technologies*, Vol. 8 N. 2/3, p. 58-76, décembre 2014. Résumé Accès : http://www.inderscience.com/info/inarticle.php?artid=66378
- Sophie Chabridon, Romain Laborde, Thierry Desprats, Arnaud Oglaza, Pierrick Marie, Samer Machara Marquez . *A survey on addressing privacy together with quality of context for context management in the Internet of Things.* Dans : *Annals of Telecommunications*, Springer, Numéro spécial *Privacy-aware electronic society*, Vol. 69 N. 1, p. 47-62, février 2014. Résumé Accès : http://link.springer.com/article/10.1007/s12243-013-0387-2 - http://oatao.univ-toulouse.fr/12723/
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *A formal model of trust for calculating the quality of X.509 certificate.* Dans : *Security and Communication Networks*, Wiley, Vol. 4 N. 6, p. 651-665, juin 2011. Résumé Accès : http://onlinelibrary.wiley.com/doi/10.1002/sec.198/abstract
- Romain Laborde, Michel Kamel, Ahmad Samer Wazan, François Barrère, Abdelmalek Benzekri. *A secure collaborative web-based environment for virtual organisations.* Dans : *International Journal of Web Based Communities*, Inderscience Publishers, Numéro spécial *Dynamic Virtual Communities in the Information Society*, Vol. 5 N. 2, p. 273-292, 2009.
- Michel Kamel, Romain Laborde, François Barrère, Abdelmalek Benzekri. *A trust-based virtual collaborative environment.* Dans : *Journal of Digital Information Management*, Digital Information Research Foundation (DIRF), Vol. 6 N. 5, (en ligne), octobre 2008. Résumé Accès : http://www.dirf.org/jdim/v6n506.pdf
- D.W. Chadwick, G. Zao, O. Otenko, Romain Laborde, L. Su. *PERMIS: A Modular Authorization Infrastructure.* Dans : *Concurrency and Computation:Practice and Experience*, Wiley, Numéro spécial *UK e-Science All Hands Meeting 2006*, Vol. 20 N. 11, p. 1341-1357, 2008.

- D.W. Chadwick, L. Su, Romain Laborde. *Providing Secure Coordinated Access to Grid Services.* Dans : *Concurrency and Computation:Practice and Experience*, Wiley, Numéro spécial *Middleware for Grid Computing*, Vol. 20 N. 9, p. 1071-1094, 2008.
- Romain Laborde, Michel Kamel, François Barrère, Abdelmalek Benzekri. *Implementation of a Formal Security Policy Refinement Process in WBEM Architecture.* Dans : *Journal of Network and Systems Management*, Springer, Vol. 15 N. 2, p. 241-266, juin 2007.
  Résumé Accès : http://dx.doi.org/10.1007/s10922-007-9063-z
- Romain Laborde, François Barrère, Abdelmalek Benzekri. *Network Security Policy Refinement Process: Expression and Analysis.* Dans : *Journal of High Speed Networks*, Deepinder Sidhu, Numéro spécial *Managing Security Polices: Modeling, Verification and Configuration*, Vol. 15 N. 3, p. 247-260, 2006.
  Résumé Accès : http://iospress.metapress.com/link.asp?id=bkcm65lh4y060brg

Articles de revues nationales / National journal papers

- Arnaud Oglaza, Romain Laborde, Pascale Zaraté. *KAPUER : un assistant à l'écriture de politiques d'autorisation pour la protection de la vie privée.* Dans : *Ingénierie des Systèmes d'Information*, Hermès Science, Vol. 19, N. 6, p. 91-115, décembre 2014.
- Abdelmalek Benzekri, François Barrère, Romain Laborde. *Gestion des habilitations : modèles et architectures.* Dans : *Revue de l'Electricité et de l'Electronique*, Société de l'Electricité, de l'Electronique et des Technologies de l'Information et de la Communication (SEE), Paris, Vol. 2013, N. 4, p. 35-41, octobre 2013.
  Résumé Accès : http://oatao.univ-toulouse.fr/12734/

Contributions à des ouvrages de synthèse / Book chapters

- Michel Kamel, Abdelmalek Benzekri, François Barrère, Romain Laborde. *Securing virtual enterprise collaboration.* Dans : *Advances in Collaborative Civil Aeronautical Multidisciplinary Design Optimization*. Ernst Kesseler (Eds.), American Institute of Aeronautics and Astronautics (AIAA), p. 1-1, Progress in Astronautics and Aeronautics series, février 2010.
  Résumé Accès : http://www.aiaa.org/content.cfm?pageid=360&id=1791

Conférences et workshops internationaux / International conference papers

- Arnaud Oglaza, Romain Laborde, Pascale Zaraté, *Difficulties to enforce your privacy preferences on Android? Kapuer will help you (poster).* Dans *13th IEEE Consumer Communications and Networking Conference. (CCNC 2016)*, 2016
- Arnaud Oglaza, Romain Laborde, Pascale Zaraté, *Demonstration of Kapuer: A privacy policy manager on Android (demo paper).* Dans *13th IEEE Consumer Communications and Networking Conference. (CCNC 2016)*, 2016
- Ibrahim Yonis Omar, Romain Laborde, Ahmad Samer Wazan, François Barrère, Abdelmalek Benzekri. *G-Cloud on Openstack : Adressing access control and regulation requirements (regular paper).* Dans : *The International Symposium on Networks, Computers and Communications (ISNCC 2015)*, *Hammamat, Tunisia*, *13/05/2015-15/05/2015*, IEEExplore digital library, (support électronique), 2015
- Romain Laborde, Bashar Kabbani, François Barrère, Abdelmalek Benzekri. *An adaptive XACMLv3 policy enforcement point (regular paper).* Dans : *IEEE International Workshop on Adaptive Systems for Communication Networks (WASCOM 2014)*, *Västerås, Sweden*, *21/07/2014-25/07/2014*, IEEE Computer Society, p. 620-625, juillet 2014.
  Résumé Accès : http://dx.doi.org/10.1109/COMPSACW.2014.104
- Arnaud Oglaza, Pascale Zaraté, Romain Laborde. *KAPUER: A Decision Support System for Protecting Privacy (regular paper).* Dans : *Group Decision and Negotiation (GDN 2014)*, *Toulouse, France*, *10/06/2014-13/06/2014*, Pascale Zaraté, Gregory Kersten, Jorge Hernandez (Eds.), Springer, LNBIP 180, p. 100-107, juin 2014.
  Résumé Accès : http://oatao.univ-toulouse.fr/13069/
- Bashar Kabbani, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Specification and Enforcement of Dynamic Authorization Policies oriented by Situations (regular paper).* Dans : *IFIP International Conference on New Technologies, Mobility and Security (NTMS 2014)*, *Dubai, UAE*, *30/03/2014-02/04/2014*, IEEE Communications Society, p. 1-6, avril 2014.
  Résumé Accès : http://dx.doi.org/10.1109/NTMS.2014.6814050
- Abdelmalek Benzekri, François Barrèrre, Romain Laborde, Bashar Kabbani. *Managing Dynamic Authorization (regular paper).* Dans : *Workshop on Code, Cryptography and Communication Systems*, *Meknes, Morocco*, *07/11/2013-08/11/2013* (conférencier invité), Ecole Supérieure de Technologie, (en ligne), novembre 2013 (keynote speaker).
  Résumé Accès : www.irit.fr/lien-a-venir

- Hicham El Khoury, Romain Laborde, François Barrère, Abdelmalek Benzekri, Maroun Chamoun. *Specification Method for Analyzing Fine Grained Network Security Mechanism Configurations (short paper)*. Dans : *Symposium on Configuration Analytics and Automation (SafeConfig 2013)*, *Washington, D.C., USA*, *16/10/2013*, IEEE, p. 483-487, 2013.
  Résumé Accès : http://dx.doi.org/10.1109/CNS.2013.6682764 - http://oatao.univ-toulouse.fr/12724/
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri, D.W. Chadwick. *PKI Interoperability: Still an Issue? A Solution in the X.509 Realm (regular paper)*. Dans : *World Conference on Information Security Education*, *Auckland, New Zealand*, *08/07/2013-10/07/2013*, Vol. 406, Springer Berlin / Heidelberg, IFIP Advances in Information and Communication Technology, p. 68-82, juillet 2013.
  Résumé Accès : http://link.springer.com/chapter/10.1007/978-3-642-39377-8_8
- Arnaud Oglaza, Romain Laborde, Pascale Zaraté. *Authorization policies: Using Decision Support System for context-aware protection of user's private data (regular paper)*. Dans : *IEEE International Symposium on UbiSafe Computing*, *Melbourne (Australia)*, *16/07/2013-18/07/2013*, IEEExplore digital library, p. 1639-1644, juillet 2013.
  Accès : http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6681028 - http://oatao.univ-toulouse.fr/12520/
- Romain Laborde, François Barrère, Abdelmalek Benzekri. *Toward Authorization as a Service: A Study of the XACML Standard (regular paper)*. Dans : *Communications and Networking Symposium*, *San Diego, California, USA*, *07/04/2013-10/04/2013*, Vol. 45, Hassan Rajaei, Abdolreza Abhari (Eds.), Curran Associates, Inc., Simulation Series 3, p. 55-61, avril 2013.
  Résumé Accès : http://dl.acm.org/citation.cfm?id=2499995 - http://oatao.univ-toulouse.fr/12467/
- Jean-Paul Arcangeli, Amel Bouzeghoub, Valérie Camps, Marie-Françoise Canut, Sophie Chabridon, Denis Conan, Thierry Desprats, Romain Laborde, Emmanuel Lavinal, Sébastien Leriche, Hervé Maurel, André Péninou, Chantal Taconet, Pascale Zaraté. *INCOME - Multi-scale Context Management for the Internet of Things (regular paper)*. Dans : *International Joint Conference on Ambient Intelligence*, *Pisa, Italy*, *13/11/2012-15/11/2012*, Vol. 7683, Fabio Paterno, Boris de Ruyter, Panos Markopoulos, Evert van Loenen, Kris Luyten (Eds.), Springer, Lecture Notes in Computer Science, p. 338-347, novembre 2012.
  Accès : http://dx.doi.org/10.1007/978-3-642-34898-3
- Hicham El Khoury, Romain Laborde, Maroun Chamoun, François Barrère, Abdelmalek Benzekri. *A Generic Attribute-Based Model for Network Security Mechanisms Representation and Configuration (regular paper)*. Dans : *International Conference on Frontier of Computer Science and Technology (FCST 2012)*, *Suzhou, China*, *21/11/2012-23/11/2012*, Soochow University, (support électronique), novembre 2012.
- François Barrère, Romain Laborde, Abdelmalek Benzekri. *Designing and deploying a secured VO for a wine geotraceability application (regular paper)*. Dans : *International Conference on Security and Management (SAM 2012)*, *Las Vegas, USA*, *16/07/2012-19/07/2012*, Vol. ISBN: 1-60132-203-8, CSREA press, p. 1-7, 2012.
  Résumé Accès : http://elrond.informatik.tu-freiberg.de/papers/WorldComp2012/SAM9747.pdf
- Hicham El Khoury, Romain Laborde, François Barrère, Maroun Chamoun, Abdelmalek Benzekri. *A Formal Data Flow-Oriented Model For Distributed Network Security Conflicts Detection (regular paper)*. Dans : *International Conference of Networking and Services (ICNS 2012)*, *St. Maarten, The Netherlands Antilles*, *25/03/2012-30/03/2012*, Xpert Publishing Service (XPS), p. 20-27, 2012.
  Résumé Accès : http://www.thinkmind.org/index.php?view=article&articleid=icns_2012_1_40_10088
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *The X.509 trust model needs a technical and legal expert (regular paper)*. Dans : *Workshop on Telecommunications: From Research to Standards (ICC'12 WS 2012)*, *Ottawa*, *10/06/2012-11/06/2012*, IEEExplore digital library, p. 6895-6900, juin 2012.
  Accès : http://dx.doi.org/10.1109/ICC.2012.6364860
- Hicham El Khoury, Romain Laborde, François Barrère, Abdelmalek Benzekri, Maroun Chamoun. *A Generic Data Flow Security Model (poster)*. Dans : *Symposium on Configuration Analytics and Automation (SafeConfig 2011)*, *Arlington, VA, USA*, *31/10/2011-01/11/2011*, IEEE, p. 1-2, 2011.
  Accès : http://dx.doi.org/10.1109/SafeConfig.2011.6111671
- Marwan Cheaito, Romain Laborde, François Barrèrre, Abdelmalek Benzekri. *A deployment framework for self-contained policies (regular paper)*. Dans : *IEEE/IFIP International Conference on Network and Service Management (CNSM 2010)*, *Niagara Falls -CANADA*, *25/10/2010-29/10/2010*, IEEE Communications Society, p. 88-95, janvier 2011.
  Résumé Accès : http://dx.doi.org/10.1109/CNSM.2010.5691328
- Romain Laborde, Marwan Cheaito, François Barrère, Abdelmalek Benzekri. *Toward self-contained authorization policies (short paper)*. Dans : *IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY 2010)*, *Fairfax, Virginia Northern, USA*, *21/07/2010-23/07/2010*, IEEE Computer Society, p. 103-106, 2010.
- Romain Laborde, Marwan Cheaito, François Barrèrre, Abdelmalek Benzekri. *An extensible XACML authorization web service: Application to dynamic web sites access control (regular paper)*. Dans : *Workshop on Security and Privacy in Telecommunications and Information Systems (SePTIS 2009)*, *Marrakech, Morocco*, *29/11/2009-04/12/2009*, IEEE Computer Society, p. 499-505, 2009.
- Marwan Cheaito, Romain Laborde, François Barrère, Abdelmalek Benzekri. *An extensible XACML authorization decision engine for context aware applications (regular paper)*. Dans : *International Conference on Pervasive Computing and Applications (ICPCA 2009)*, *Tamkang University -Taiwan*, *03/12/2009-05/12/2009*, IEEE, (support électronique), décembre 2009.

- Michel Kamel, Romain Laborde, François Barrère, Abdelmalek Benzekri. *An organizational pattern for contributing to the deployment of secure Virtual Enterprises (regular paper).* Dans : *International Conference on Security and Management (SAM 2009)*, *Monte Carlo Resort, Las Vegas, Nevada, USA*, *13/07/2009-16/07/2009*, Vol. Volume 1, Hamid R. Arabnia (Eds.), University of Georgia, p. 56-61, juillet 2009.
- Michel Kamel, Romain Laborde, François Barrère, Abdelmalek Benzekri. *SecMaLET: a tool for establishing the chain of trust within a Virtual Enterprise (regular paper).* Dans : *IFIP Network and Service Security Conference (N2S 2009)*, *Paris - FRANCE*, *24/06/2009-26/06/2009*, Pascal Urien, Guy Pujolle (Eds.), IFIP, (support électronique), juin 2009.
- Ahmad Samer Wazan, Romain Laborde, D.W. Chadwick, François Barrère, Abdelmalek Benzekri. *Which Web Browsers Process SSL Certificates in a Standardized Way?* Dans : *IFIP TC-11 International Information Security Confernce (IFIP SEC 2009)*, *Cyprus*, *18/05/2009-20/05/2009*, Springer, p. 432-442, mai 2009. Résumé Accès : http://www.irit.fr/publis/SIERA/SSL-SEC2009.pdf
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *The X.509 certificate quality.* Dans : *IEEE International Conference on Digital Information Management (ICDIM 2008)*, *Londres*, *13/11/2008-16/11/2008*, IEEE, p. 928-930, 2009.
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Validating X.509 Certificates Based on Their Quality.* Dans : *International Symposium on Trusted Computing*, *ZhangJiaJie, China*, *18/11/2008-21/11/2008*, IEEE Computer Society, p. 2055-2060, 2008.
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Authentication in Virtual Organizations: a Reputation Based PKI Interconnection Model.* Dans : *International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and New Technologies*, *Munich, Germany*, *21/10/2008-22/10/2008*, Vol. 18, Springer, Communications in Computer and Information Science, p. 84-95, octobre 2008.
- Romain Laborde, Thierry Desprats. *An Extension of XACML to Improve the Performance of Decision Making Processes when Dealing with Stable Conditions.* Dans : *International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and New Technologies*, *Munich, Germany*, *21/10/2008-22/10/2008*, Vol. 18, Springer, Communications in Computer and Information Science, p. 13-24, octobre 2008.
- Michel Kamel, Romain Laborde, Abdelmalek Benzekri, François Barrère. *A best practices-oriented approach for establishing trust chains within Virtual Organisations.* Dans : *International Workshop on Security and Privacy in Enterprise Computing (InSPEC 2008)*, *Munich, Germany*, *15/09/2008-15/09/2008*, IEEE, (support électronique), 2008.
- Romain Laborde, Michel Kamel, François Barrère, Abdelmalek Benzekri. *PEP = Point to Enhance Particularly.* Dans : *IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2008)*, *IBM Palisades, 334 Route 9W, Palisades, NY 10964, USA*, *02/06/2008-04/06/2008*, IEEE Computer Society, p. 93-96, 2008.
- Romain Laborde, Thierry Desprats. *Dealing with Stable Environmental Conditions in XACML Systems.* Dans : *International Conference on Systems and Networks Communications (ICSNC 2007)*, *Cap Esterel, French Riviera, France*, *25/08/2007-31/08/2007*, IEEE Computer Society, p. 63-69, septembre 2007.
- Romain Laborde, Michel Kamel, François Barrère, Abdelmalek Benzekri. *A secure collaborative web based environment for virtual organizations.* Dans : *International Workshop on Dynamic Virtual Communities : From Connectivity to Information Society*, *INSA de LYON, FRANCE*, *29/10/2007-29/10/2007*, IEEE, p. 723-730, 2007.
- Michel Kamel, Romain Laborde, Abdelmalek Benzekri, François Barrère. *Virtual Organizations: An ISO/IEC 17799-based tool for evaluating the maturity level of the organizations security practices.* Dans : *Latin American Network Operations and Management Symposium (LANOMS 2007)*, *petropolis - Brasil*, *10/09/2007-12/09/2007*, Vol. IEEE Catalog Number: 07EX1769, IEEE, ISBN: 1-4244-1182-3 Library of Congress: 200792390, (support électronique), septembre 2007.
- Michel Kamel, Abdelmalek Benzekri, François Barrère, Romain Laborde. *Evaluating the conformity of an access control architecture for Virtual Organizations with ISO/IEC 17799.* Dans : *IEEE International Global Information Infrastructure Symposium (GIIS 2007)*, *Marrakech - Morocco*, *02/07/2007-06/07/2007*, Nazim Agoulmine, Raouf Boutaba, Ahmed Serhrouchni (Eds.), IEEE, ISBN 1-4244-1375-3, p. 173-180, 2007.
- Michel Kamel, Abdelmalek Benzekri, François Barrère, Romain Laborde. *Evaluating the Virtual Organizations security solutions using the ISO/IEC 17799 standard.* Dans : *International Conference on Concurrent Enterprising (ICE 2007)*, *Sophia-Antipolis, FRANCE*, *04/06/2007-06/06/2007*, Pawar Kulwant, Marc Pallot, Thoben Klaus-Dieter (Eds.), Centre for Concurrent Enterprise, University Business School, ISBN 978 0 85358 233 5 , p. 269-276, juin 2007.
- D.W. Chadwick, Wensheng Xu, O. Otenko, Romain Laborde, Bassem Nasser. *Multi-session Separation of Duties (MSoD) for RBAC.* Dans : *International Workshop on Security Technologies for Next Generation Collaborative Business Applications (SECOBAP 2007)*, *Istanbul, Turkey*, *20/04/2007-20/04/2007*, IEEE, (en ligne), 2007. Résumé Accès : http://www.ieee.org/web/publications/procieee/
- D.W. Chadwick, L. Su, Romain Laborde. *Providing secure coordinated access to grid services.* Dans : *International Workshop on Middleware for Grid Computing (MGC 2006)*, *Melbourne, Australia*, *27/11/2006-01/12/2006*, ACM Press, p. 1-1, 2006. Résumé Accès : http://doi.acm.org/10.1145/1186675.1186677

- D.W. Chadwick, G. Zao, O. Otenko, Romain Laborde, L. Su. *Building a Modular Authorization Infrastructure.* Dans : *UK e-Science All Hands Meeting (AHM 2006)*, *Nottingham UK*, *18/09/2006-21/09/2006*, NeSC, (en ligne), 2006.
  Résumé Accès : http://www.allhands.org.uk/2006/proceedings/papers/677.pdf
- D.W. Chadwick, L. Su, O. Otenko, Romain Laborde. *Co-ordination between Distributed PDPs.* Dans : *IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2006)*, *University of Western Ontario, London , Canada*, *05/06/2006-07/06/2006*, IEEE, p. 163-172, 2006.
  Résumé Accès : http://doi.ieeecomputersociety.org/10.1109/POLICY.2006.14
- Bassem Nasser, Romain Laborde, Abdelmalek Benzekri, François Barrère, Michel Kamel. *Dynamic creation of inter-organizational grid Virtual Organizations.* Dans : *1st IEEE International conference on eScience and Grid Computing*, *Australia*, *05/12/2005-08/12/2005*, //to appear in the proceedings, décembre 2005.
  Résumé Accès : http://www.gridbus.org/escience/index.html
- Bassem Nasser, Romain Laborde, Abdelmalek Benzekri, François Barrère, Michel Kamel. *Access Control Model for Inter-organizational Grid Virtual Organizations.* Dans : *On the Move to Meaningful Internet Systems 2005: OTM 2005 workshops. MIOS+Interop Workshop*, *Cyprus*, *31/10/2005-01/11/2005*, Robert Meersmann, Zahir Tari, Pilar Herrero (Eds.), Springer-Verlag Berlin Heidelberg 2005, p. 537, octobre 2005.
- Bassem Nasser, Romain Laborde, François Barrère, Abdelmalek Benzekri, Michel Kamel. *A framework for dynamic creation of grid Virtual Organizations.* Dans : *Simposio Seguranca em Informatica (SSI 2005)*, *Brésil*, *08/11/2005-11/11/2005*, Paulo Sérgio Motta Pires, Clovis Torres Fernandes (Eds.), Technological Institute of Aeronautics (ITA) Airspace Technical Center (CTA), (support électronique), novembre 2005.
- Bassem Nasser, Abdelmalek Benzekri, Romain Laborde, Frédéric Grasset, François Barrère. *Access Control Model for Grid Virtual Organizations.* Dans : *International Conference on Enterprise Information Systems*, *Miami, USA*, *25/05/2005-28/05/2005*, Chen Chin-Sheng , Filipe Joaquim , Seruca Isabel , Cordeiro José (Eds.), 972-8865-19-8, p. 152-158, mai 2005.
- Romain Laborde, François Barrère, Abdelmalek Benzekri. *A formal framework (Expression + Analysis) for network security mechanisms configuration.* Dans : *4th IEEE International Symposium onNetwork Computing and Applications (IEEE NCA05)*, *Cambridge, MA, USA*, *27/07/2005-29/07/2005*, IEEE Computer Society, ISBN 0-7695-2326-9, juillet 2005.
- Romain Laborde, Michel Kamel, François Barrère, Abdelmalek Benzekri. *Implementation of a formalsecurity policy refinement process in WBEM architecture.* Dans : *4th Latin American Network Operations and Management Symposium (LANOMS 2005)*, *Porto Alegre*, *29/08/2005-31/08/2005*, ISBN 85-76690-38-1, p. 65-76, août 2005.
- Romain Laborde, François Barrère, Abdelmalek Benzekri. *A security management information model derivation framework: from goals to configurations.* Dans : *3rd international Workshop on Formal Aspects in Security and Trust (FAST2005)*, *Newcastle Upon Tyne*, *18/07/2005-19/07/2005*, Springer, p. 215-232, juillet 2005.
- Romain Laborde, Bassem Nasser, Frédéric Grasset, François Barrère, Abdelmalek Benzekri. *A formal approach for the evaluation of network security mechanisms based on RBAC policies.* Dans : *2nd International Workshop on Security Issueswith Petri Nets and other Computational Models (WISP'04)*, *Bologna, Italy*, Electronic Notes in Theoretical Computer Science, Volume 121, Elsevier, p. 117-142, juin 2004.
  Résumé Accès : http://dx.doi.org/10.1016/j.entcs.2004.10.011
- Romain Laborde, Bassem Nasser, Frédéric Grasset, François Barrère, Abdelmalek Benzekri. *Network Security Management: A Formal Evaluation Tool based on RBAC Policies.* Dans : *IFIP NetCon'2004*, *Palma de Mallorca, Spain*, *03/11/2004-05/11/2004*, D. Gaïti, S. Galmés, R. Puigjaner (Eds.), Springer ISBN 0-387-23197-8, p. 69-80, novembre 2004.
- Romain Laborde, Bassem Nasser, Frédéric Grasset, François Barrère, Abdelmalek Benzekri. *A formal tool for user based network security policy specification.* Dans : *International Workshop Security Analysis of Systems: Formalisms and Tools (SASYFT'04)*, *Orléans, France*, *21/06/2004-22/06/2004*, Laboratoire d'Informatique Fondamentale d'Orléans, 4, rue Léonard de Vinci, BP 6759, F45067 Orléans cedex2, France - Technical Report N°2004-11, p. 1-18, juin 2004.
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde, Bassem Nasser. *SPIDERNet : the Security Policy Derivation for Networks tool.* Dans : *3rd IEEE Latin America Network Operations and Management Symposium (LANOMS)*, *Iguaçu, Brazil*, *04/09/2003-06/09/2003*, Edmundo R. M. Madeira and Elias P. Duarte Jr., p. 29-36, septembre 2003.
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde, Bassem Nasser. *Négociation de la politique de sécurité Inter-Domaines.* Dans : *SAR 2003 CONFERENCE FRANCOPHONE SECURITE ET ARCHITECTURE*, *Marrakech Maroc* , *30/06/2003-04/07/2003*, I. CHRISMENT - R. DSSOULI, INRIA Domaine de Voluceau - Roquencourt - BP 105 - 78153 Le Chesnay Cédex FRANCEDépot Légal: 200503 / 110ISBN 2 - 7261 - 1251 - X, p. 21-31, juin 2003.
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde, Bassem Nasser. *Inter-Domains policy negociation.* Dans : *Policy 2003, Fourth International Workshop Policies for Distributed Systems and Networks - IEEE*, *Lake Como, Italy*, *04/06/2003-06/06/2003*, IEEE Computer Society, IEEE Computer Society Customer Service Center 10662 Los Vaqueros Circle P.O. Box 3014 Los Alamitos, CA 90720-1314, p. 239-242, juin 2003.
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde. *A Multi-Domain Security Policy Distribution Architecture for Dynamic IP Based VPN Management.* Dans : *Third International Workshop Policies for Distributed Systems and Networks - IEEE*, *Monterey, California, USA*, *05/06/2002-07/06/2002*, IEEE Computer

Society - ISBN 0-7695-1611-4, IEEE Computer SocietyCustomer Service Center10662 Los Vaqueros CircleP.O. Box 3014Los Alamitos, CA 90720-1314, p. 224-227, juin 2002.

- Abdelmalek Benzekri, François Barrère, Frédéric Grasset, Romain Laborde, Yves Raynaud. *A security Policy Management Architecture for the Extended Enterprise.* Dans : *7th International Conference on Concurrent Enterprising*, *Bremen, Germany*, *27/06/2001-29/06/2001*, Klaus-Dieter Thoben, Frithjof Weber & Kulwant S Pawar, Centre for Concurrent Enterprising, University of Nottingham, UKISBN 0 85358 098 7, p. 181-186, juin 2001.
  Accès : http://www.ice-2001.org

Conférences et workshops nationaux / National conference papers

- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Etude du concept de confiance pour les infrastructures à clés publiques (regular paper).* Dans : *Gestion de REseaux et de Services (GRES 2014)*, *Paris*, *01/12/2014-03/12/2014*, IEEExplore digital library, (support électronique), 2015.
- Jean-Paul Arcangeli, Sophie Chabridon, Denis Conan, Thierry Desprats, Romain Laborde, Sébastien Leriche, Léon Lim, Chantal Taconet, Raja Boujbel, Samer Machara Marquez , Pierrick Marie, Sam Rottenberg. *Gestion de contexte multi-échelle pour l'Internet des objets (regular paper).* Dans : *Journées francophones Mobilité et Ubiquité (UBIMOB 2014)*, *Sophia Antipolis*, *05/06/2014-06/06/2014*, Laboratoire i3S, (en ligne), 2014. Résumé Accès : http://ubimob2014.sciencesconf.org/39139/document - http://oatao.univ-toulouse.fr/13105/
- Jean-Paul Arcangeli, Amel Bouzeghoub, Valérie Camps, Sophie Chabridon, Denis Conan, Thierry Desprats, Romain Laborde, Emmanuel Lavinal, Sébastien Leriche, Hervé Maurel, Mohamed Mbarki, André Péninou, Chantal Taconet, Pascale Zaraté, Raja Boujbel, Léon Lim, Samer Machara Marquez , Pierrick Marie, Clément Mignard, Arnaud Oglaza, Sam Rottenberg. *Projet INCOME : INfrastructure de gestion de COntexte Multi-Echelle pour l'Internet des Objets (short paper).* Dans : *Conférence Francophone sur les Architectures Logicielles (CAL 2014)*, *Paris*, *10/06/2014-11/06/2014*, ENSEEIHT, (en ligne), juin 2014. Résumé Accès : http://cal2014.enseeiht.fr/papers/Projet%20INCOME%20INfrastucture%20de%20gestion%20de%20COntexte%20Multi-Echelle%20pour%20l%E2%80%99Internet%20des%20Objets.pdf - http://oatao.univ-toulouse.fr/13093/
- Bashar Kabbani, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Managing Break-The-Glass using Situation-oriented authorizations (regular paper).* Dans : *Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2014)*, *Saint-Germain-Au-Mont-d'Or (Lyon), France*, *13/05/2014-16/05/2014*, HAL-INRIA, (en ligne), mai 2014. Résumé Accès : http://sarssi14.liris.cnrs.fr/ressources/pdfs/sarssi2014_bkabbani.pdf - http://oatao.univ-toulouse.fr/13032/
- Jean-Paul Arcangeli, Amel Bouzeghoub, Valérie Camps, Marie-Françoise Canut, Sophie Chabridon, Denis Conan, Thierry Desprats, Romain Laborde, Sébastien Leriche, Hervé Maurel, André Péninou, Chantal Taconet, Pascale Zaraté. *Projet INCOME : INfrastructure de gestion de COntexte Multi-Échelle pour l' Internet des Objets (regular paper).* Dans : *Journées francophones Mobilité et Ubiquité (UBIMOB 2012)*, *Anglet*, *04/06/2012-06/06/2012*, Cépaduès Editions, p. 46-49, juin 2012.
- Hicham El Khoury, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Vers un modèle formel orienté flux de données pour l'analyse de politiques de sécurité réseau (regular paper).* Dans : *Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2011)*, *La Rochelle*, *18/05/2011-21/05/2011*, IEEE Computer Society - Conference Publishing Services, p. 1-7, 2011.
- Romain Laborde, Marwan Cheaito, François Barrère, Abdelmalek Benzekri. *Vers un système d' autorisation comme un service (regular paper).* Dans : *Gestion de REseaux et de Services (GRES 2010)*, *Montréal, Canada*, *13/10/2010-15/10/2010*, eFolia, (support électronique), novembre 2010. BibTeX
- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Quality of Certificate: an indicator to improve the usability of X.509 Certificates (short paper).* Dans : *Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2010)*, *Menton -France*, *18/05/2010-21/05/2010*, INRIA, (support électronique), 2010.
- Marwan Cheaito, Romain Laborde, François Barrère, Abdelmalek Benzekri. *Configurable Data Types in Policy Based Access Control Management: A Specification and Enforcement Framework (regular paper).* Dans : *Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2010)*, *Menton -France*, *18/05/2010-21/05/2010*, INRIA, (support électronique), 2010.
- Romain Laborde, Thierry Desprats. *Gestion de conditions stables dans XACML : intérêt d' une approche par notification.* Dans : *Gestion de REseaux et de Services (GRES 2007)*, *Hammamet,Tunisie*, *06/11/2007-09/11/2007*, Sami Tabbane, Choukair Zied (Eds.), Hermès Science, 978-2-7462-2273-1, p. 161-168, décembre 2008. Résumé Accès : http://www.irit.fr/publis/SIERA/gres2007-desprats-laborde-Soumission.pdf
- Michel Kamel, François Barrère, Romain Laborde, Abdelmalek Benzekri. *Un environnement de collaboration sécurisé pour les organisations virtuelles.* Dans : *Gestion de REseaux et de Services (GRES 2007)*, *Hammamet,Tunisie*, *06/11/2007-09/11/2007*, Sami Tabbane, Zièd Choukair (Eds.), Ecole Supérieure des Communications de Tunis, (support électronique), novembre 2007.

- Bassem Nasser, Abdelmalek Benzekri, Romain Laborde, François Barrère, Michel Kamel. *Grid Virtual Organization: Access Control Management.* Dans : *GRES05: Gestion de REseaux et de Services*, *Luchon, France*, *28/02/2005-02/03/2005*, Abdelmalek Benzekri , Michelle Sibilla (Eds.), ISBN: 2-9520326-5-3, p. 283-295, février 2005.
  Résumé Accès : http://www.irit.fr/gres05
- Romain Laborde, Bassem Nasser, Frédéric Grasset, François Barrère, Abdelmalek Benzekri. *Un Modèle et un outil d'analyse formels pour la configuration des mécanismes de sécurité réseau.* Dans : *6ème colloque francophone GRES¿2005*, *Luchon, France*, *28/02/2005-02/03/2005*, Abdelmalek. Benzekri , Michelle. Sibilla (Eds.), ISBN 2-9520326-5-3, p. 251-267, février 2005.
- Romain Laborde, Bassem Nasser, Frédéric Grasset, François Barrère, Abdelmalek Benzekri. *Une nouvelle technique pour l'évaluation formelle de mécanismes de sécurité réseaux.* Dans : *3ème Conférence sur la Sécurité et Architectures Réseaux (SAR)*, *La Londe, France*, *21/06/2004-25/06/2004*, Abdelmadjid Bouabdallah, Ahmed Serhrouchni (Eds.), X, p. 69-80, juin 2004.
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde, Bassem Nasser. *Un modèle de gestion de VPN basé sur les utilisateurs.* Dans : *Gestion de Réseaux et de Services (GRES)*, *Fortaleza, Brésil*, *24/02/2003-28/02/2003*, Joaquim Celestino Jr., p. 255-267, février 2003.
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde, Yves Raynaud. *Distribution de politiques IPSec.* Dans : *GRES 01 Gestion de Réseau et de Service4ème Colloque Francophone*, *Marrakech, Maroc*, *17/12/2001-21/12/2001*, Ecole Nationale Supérieure des TélécommunicationsGroupe des Ecoles des Télécommunications, 46 Rue Barrault 75634 Paris Cedex 13, p. 271-284, décembre 2001.

Conférences sans actes publiés / Conference papers without published proceedings

- Sophie Chabridon, Thierry Desprats, Romain Laborde, Chantal Taconet, Pascale Zaraté. *Gestion de contexte dans l'Internet des objets : analyse de l'interdépendance entre protection de la vie privée et qualité de contexte.* Dans : *Atelier sur la Protection de la Vie Privée*, *Les Loges en Josas, France*, *17/06/2013-19/06/2013*.
  Accès : http://apvp2013.prism.uvsq.fr/
- Romain Laborde. *Evaluation of the X.509 Certificates Chain of Trust.* Dans : *US France Young Engineering Scientists Symposium*, *Washington DC*, *07/07/2009-09/07/2009* (conférencier invité).
- Abdelmalek Benzekri, Bassem Nasser, Romain Laborde, Frédéric Grasset, François Barrère. *Hybrid distributed system security Case study: IMAGE middleware.* Dans : *Atelier Sécurité des Systèmes d'Information (SSI)*, *Biarritz*, *25/05/2004*.
  Résumé Accès : http://inforsid2004.univ-pau.fr/workshop.htm
- François Barrère, Abdelmalek Benzekri, Frédéric Grasset, Romain Laborde, Bassem Nasser. *Automated inter-domain security policy generation.* Dans : *11th Workshop of the HP OpenView University Association*, *Paris*, *20/06/2004-23/06/2004*.
  Résumé Accès : http://aramis.iup.univ-evry.fr:8080/~nazim/hpovua2004/HPOVUA2004.htm

Autres types de publications / Other publications

- Ahmad Samer Wazan, Romain Laborde, François Barrère, Abdelmalek Benzekri, D.W. Chadwick. *Proposition summary to X.509 committee: Adding the role of technical and juridical expert to the X.509 trust model - ITU Study group 17 - TD 0131*. avril 2013.
  Résumé Accès : http://thailandpki.org/wp-content/uploads/ITU-Proposal-X509-April2013.pdf
- D.W. Chadwick, L. Su, Romain Laborde. *Use of XACML Request Context to Obtain an Authorisation Decision*. Diffusion scientifique. novembre 2009. Open Grid Forum, OGSA Authorization WG, GFD Proposed Recommendation, P-REC 159
  Accès : http://www.ogf.org/documents/GFD.159.pdf