lina
UMR 6241

J. Christian Attiogbé
Université de Nantes
(+33 2)/(02) 51 12 58 18
christian.attiogbe@univ-nantes.fr

Nantes, le jeudi 8 décembre 2016

Rapport sur le mémoire de thèse présenté par
Thi-Mai Nguyen
pour l'obtention du grade de Docteur de Telecom SudParis (France)

par J. Christian Attiogbé
Professeur, Université de Nantes, Laboratoire LINA

Titre de la thèse : ***A Model driven engineering approach to build secure information systems***

Contexte du travail : La thèse a été effectuée à l'Université Paris Saclay et Télécom SudParis, sous la direction de Amel Mammar et Régine Laleau.

Structure du mémoire : Ce rapport est établi à partir du mémoire de 182 pages soumis par Thi-Mai Nguyen. Le mémoire est rédigé en anglais ; il contient **sept chapitres** dont un chapitre (Chap. 1) d'introduction et un chapitre (Chap. 7) de conclusion.

Dans la suite de ce rapport, nous faisons un résumé des chapitres contenus dans le mémoire puis une évaluation de l'ensemble des travaux.

Résumé des travaux présentés

Le **Chapitre 1** introduit le contrôle d'accès comme une des facettes de la sécurité dans les systèmes d'information. Une politique de contrôle d'accès permet de gérer les accès aux ressources par les usagers du système. Un des principaux défis étant la prise en compte des exigences de sécurité le plus tôt possible dans les phases de développement des systèmes. Un des défis auxquels s'attaque la thèse est la séparation de la prise en compte de la sécurité du code fonctionnel de telle sorte que le système final soit plus facile à maintenir, alors que dans des approches existantes la gestion de la sécurité est mêlée avec les aspects fonctionnels. Une approche basée sur la programmation par Aspects est choisie à cet effet. Un autre défi attaqué est la prise en compte, en termes de modélisation et de vérification, des règles de sécurité dynamiques liant dans le temps les actions d'un système.

Ce chapitre résume aussi les contributions de la thèse en trois points : i) la spécification graphique des modèles de sécurité à l'aide de diagrammes de classe UML, de SecureUML et des diagrammes d'activités de UML pour les règles de sécurité dynamique ; ii) la définition de règles de traduction des diagrammes UML vers des niveaux plus abstraits en B, en distinguant les parties liées à la sécurité des parties liées au fonctionnel ; iii) l'outillage de la chaîne de transformation permettant de passer des spécifications à base de notations UML aux modèles formels en B ; puis de passer des modèles B à un code orienté Aspects.

Le **Chapitre 2** est consacré à l'introduction des différents concepts utilisés dans le reste des chapitres, autour de la méthode B, de l'ingénierie dirigée par les modèles, du contrôle d'accès basé sur les rôles, et de la programmation par aspects.

Le **Chapitre 3** est consacré à un état de l'art sur les travaux traitant la sécurité des systèmes d'information. Il explore : les techniques de spécification des exigences de contrôle d'accès et les outils associés, les méthodes de transformation des politiques de contrôle d'accès basé sur les rôles (RBAC) en code, et les travaux qui traitent la sécurité à travers la programmation par aspects.

Une première partie de ce chapitre est consacrée aux techniques de spécification de la sécurité orientées modèles à états tels que UML, Alloy, Z et B.

Deux outils ont été présentés : l'outil SecureMOVA autour du formalisme SecureUML, et l'outil B4MSecure qui combine des étapes de modélisation de la sécurité en SecureUML puis la traduction en B de modèles de sécurite écrits en UML.

SecureMOVA permet de formaliser des contraintes de contrôle d'accès à l'aide du langage OCL et de pouvoir écrire ensuite des requêtes OCL à propos des usagers, des rôles, des permissions, des actions ; ainsi SecureMOVA permet d'analyser des contraintes de sécurité à travers des requêtes formulées. B4MSecure (développé dans le laboratoire LIG de Grenoble) a pour particularité d'intégrer les modèles fonctionnels et les modèles de sécurité via le contrôle d'accès. Ici les modèles fonctionnels (UML) et de contrôle d'accès (SecureUML) sont traduits en modèle formel B afin d'être vérifiés (avec les outils de preuve et d'animation disponibles en B).

Il s'en suit que ces techniques et outils ne permettent de traiter que la partie statique des informations du contrôle d'accès et des affectations des rôles aux usagers. Leur limitation est donc la prise en compte de la partie dynamique des exigences de sécurité ; il s'agit des exigences qui ont besoin de l'historique des actions.

Une partie de ce chapitre est consacrée à l'implantation des techniques de contrôle d'accès dans le développement des applications. Généralement les aspects relevant de la sécurité sont mêlés avec les autres aspects fonctionnels de l'implantation des applications. Il y a cependant des travaux qui ont utilisé des techniques de programmation par aspects pour prendre en compte la sécurité. La limitation relevée ici est que la validation des modèles considérés n'est faite qu'au niveau syntaxique entre les modèles fonctionnels et de contrôle d'accès.

Ce chapitre explore aussi d'autres techniques d'implantation du contrôle d'accès telles que cela est fait en Java (avec JAAS de Sun), les techniques d'annotations des classes et méthodes par des rôles autorisés et les techniques basées sur la programmation par Aspects.

Il s'en suit que malgré la flexibilité apportée, les techniques orientées aspects ne considèrent pas non plus les exigences dynamiques.

Le **Chapitre 4** constitue le premier axe des contributions de la thèse. Il s'agit d'une extension d'un article publié dans la conférence HASE'2016 et il traite du développement formel d'un filtre de contrôle d'accès. Une étude de cas est présentée (un système bancaire proposant des opérations sur des comptes bancaires par des usagers). La modélisation sous forme graphique des exigences de sécurité est faite à l'aide de SecureUML complétée par des diagrammes d'activités qui permettent de prendre en compte des contraintes de sécurité ou règles dynamiques. A partir de ce modèle, une traduction appropriée en B est faite afin de procéder à la vérification du modèle en B.

Ici, les apports de la thèse concernent : i) la définition d'un ensemble de règles génériques pour relier des diagrammes SecureUML des parties statiques et des diagrammes UML représentant des règles de sécurité dynamiques à une spécification B ; ii) la spécification générique d'un filtre qui permet de coordonner toutes les règles de sécurité. Un filtre est une opération qui décide en fonction des cas analysés, l'action effective à entreprendre ou non sans violer les règles de sécurité.

Pour tenir compte des besoins des règles de sécurité liées à la dynamique des actions, l'historique des actions a été explicitement introduite dans la spécification/traduction B afin de pouvoir gérer les contraintes d'ordre d'enchaînement des actions. Les actions éffectuées (l'historique) par un utilisateur dans un système sont ainsi mémorisées. Lorsqu'une action est contrainte par d'autres actions, on peut ainsi observer l'historique avant de décider de la faire ou non. Sur ce principe un ensemble de règles de traduction des contraintes de sécurité a été défini et formalisé en B, en prenant la précaution de les séparer des spécifications des actions qui représentent les fonctionnalités. Dans la mise en œuvre en B, une combinaison progressive de machines abstraites permet de séparer les opérations du niveau fonctionnel des opérations de vérification des accès. Une architecture globale de l'étude de cas traitée est donnée. La vérification du modèle B obtenu par traduction est faite avec l'outil support AtelierB.

Le **Chapitre 5** est dédié à l'outillage de la génération d'un filtre sûr pour le contrôle d'accès. Ce chapitre est une extension d'un article publié dans la conférence RCIS'2016.

Les apports de cette partie du travail concernent la traduction des modèles graphiques autour de UML vers le modèle formel en B. Le chapitre présente un aperçu de l'outil puis de la méthode B avant d'introduire une étude de cas (un système de santé : gestion de l'admission de patients dans un hopital et suivi des soins), ensuite de présenter les techniques de traduction des différentes parties (diagrammes de classe, diagramme SecureUML, diagrammes d'activités UML) en B et enfin la spécification d'un filtre sûr.

Un filtre sûr (est une opération qui) permet de restreindre l'accès à un système aux seuls usagers autorisés.

L'outil proposé ici est une extension de l'outil B4MSecure en comblant des lacunes identifiées (non prise en compte des règles de sécurité liées à la dynamique, manque de traduction de certains concepts à partir de UML, difficulté de la traduction de certaines parties des modèles SecureUML).

L'étude de cas du système de santé, a été analysée et spécifiée avec l'outil B4MSecure, les deux catégories de règles (statique et dynamique) ont été identifiées pour les modéliser soit avec SecureUML soit avec les diagrammes d'activités. Le modèle graphique global est ensuite systématiquement traduit en B, en considérant chacun de ses composants (fonctionnels, règles de sécurité statique et règle de sécurité dynamique). Ces traductions ont été possibles par l'introduction de nouvelles règles de mise en correspondance entre les concepts des modèles UML et B. Toute cette chaîne de traitement (de traduction) a été automatisée en exploitant des outils d'ingénierie de modèles disponibles dans la plateforme Topcased.

Le **Chapitre 6** du mémoire de thèse présente une approche formelle pour dériver une implantation à base d'aspects, d'un filtre sûr de contrôle d'accès.

Ce chapitre complète les résultats présentés précédemment sur la construction de filtre de contrôle d'accès en visant cette fois-ci une implantation spécifique orientée aspects. Une étude de cas concernant un système d'achats de produits (où les gestionnaires et les administratifs ont des droits spécifiques) sert ici de support.

La spécification obtenue par traduction à partir des modèles SecureUML et UML est d'abord transformée en une implantation de style relationnel par des étapes de raffinement. Cette implantation est ensuite transformée en une implantation AspectJ avec une couche de bases de données relationnelles.

La première partie du chapitre reprend la construction de filtre de contrôle d'accès comme précédemment. Le chapitre se poursuit plus spécifiquement avec l'implantation en AspectJ.

Les apports de ce chapitre sont : i) la définition d'une transformation du modèle B en implantation Java/AspectJ incluant des requêtes de création d'une base de données, des rôles, des utilisateurs et d'exécution des droits; ii) l'extension de l'outil introduit précédemment par le support de génération de l'implantation AspectJ.

Les règles de transformation des éléments de spécification B en Java/SQL sont décrites. La transformation des spécifications B issues des diagrammes de classe en JAVA/SQL permet de créer des tables de la base de données et des procédures stockées. Les opérations à sécuriser, issues des diagrammes de classe et qui apparaissent dans le modèle SecureUML sont transformées en procédures stockées. Les exigences de sécurité contenues dans les diagrammes SecureUML sont elles, utilisées pour créer les usagers, leurs rôles et permissions, en utilisant le système d'authentification de SQL Server. Finalement les exigences de sécurité contenues dans les spécifications B issues des diagrammes d'activités sont traduites en tables SQL et en méthodes JAVA permettant de les manipuler.

Après la traduction des différents constituants de la spécification B, le filtre de contrôle d'accès est obtenu sous forme d'un *advice*. La dernière partie de ce chapitre présente l'extension de l'outil support pour générer l'implantation AspectJ. La présentation et les possibilités de l'outil sont illustrés avec l'exemple du système d'achat.

Le **Chapitre 7** est la conclusion finale du mémoire de thèse. Il résume les contributions de la hèse et présente des perspectives de travail qui se dessinent après cette thèse.

Evaluation du mémoire

Le document de thèse est bien structuré et bien écrit. Les principaux chapitres sont les chapitres 4, 5 et 6. La problématique est précisément exposée et l'état de l'art pertinent.

Le positionnement des travaux sur la prise en compte des règles de sécurité dynamiques est judicieuse ; les solutions apportées via l'extension de résultats et d'outils existants constituent une bonne démarche qui a permis d'apporter de nouveaux résultats aussi bien sur la modélisation des propriétés que sur la validation de systèmes de contrôle d'accès à travers la méthode B et ses outils de preuve. Plusieurs études de cas ont été utilisées tout au long des chapitres ; cela a permis de confirmer les solutions proposées et cela facilite aussi la lecture de la thèse.

Le travail effectué est très important. Une petite dose de formalisation des règles de traduction aurait pu souligner davantage la pertinence des contributions. Le parti pris de ne pas expliciter les résultats pratiques d'expérimentation en B (les difficultés éventuelles et les statistiques de preuve) soulève des interrogations.

Les contributions de la thèse se situent à différents niveaux et concernent :

- la prise en compte des exigences dynamiques des règles de contrôle d'accès ;
- la dérivation de spécifications B et la synthèse de filtre de contrôle d'accès à partir des modèles SecureUML/UML pour des objectifs de vérification formelle ;
- la dérivation d'une implantation orientée Aspect afin de séparer les préoccupations de sécurité des fonctionnelles, et de faciliter ainsi la maintenance ;
- les outils supports développés pour accompagner les expérimentations sur des études de cas.

Les perspectives listées en fin du document sont intéressantes ; plus particulièrement, l'automatisation d'une partie des raffinements des modèles B me semble un sujet à forte priorité.

Les résultats de la thèse ont été publiés dans deux conférences internationales de grande qualité *(HASE'2016* et *RCIS'2016)*.

Au vu de ce mémoire très bien rédigé et des contributions présentées, nous constatons que Thi-Mai Nguyen a mené avec rigueur son travail de thèse ; ce travail a abouti à de nouveaux résultats ; nous considérons que cette thèse est digne d'être soutenue en vue de l'obtention du Doctorat en Informatique de Telecom SudParis.

Nantes, le 8 Décembre 2016

J. Christian Attiogbé