Résumé

Le projet SELKIS a pour objectif de développer une méthode d'analyse et conception de Systèmes d'Information (SI) sécurisés qui aborde les aspects fonctionnels et sécuritaires dès les premiers niveaux d'abstraction du développement et combine les mécanismes sécuritaires disponibles au niveau implantation dans les logiciels de stockage d'information. Cette approche convient à une grande variété de systèmes d'information et dans ce projet, elle sera appliquée à des SI médicaux. Cette méthode doit prendre en compte les propriétés de sécurité suivantes: Disponibilité, Intégrité, Confidentialité et Traçabilité qui sont cruciales dans ce type de SI.

La méthode est fondée sur une approche MDA qui permet de décrire un SI à 3 niveaux d'abstraction. Le premier niveau consiste à créer un modèle du système global (CIM), indépendant de tout aspect informatique, en considérant différents types de besoins, dont les besoins de sécurité, recueillis à partir du système à construire et de son environnement. Le second niveau décrit un modèle du système à construire indépendant de toute plateforme d'implémentation (PIM). Le dernier niveau décrit un modèle qui caractérise l'architecture d'implémentation retenue pour le SI (PSM).

L'objectif du projet est alors triple:
(i) spécifier de manière séparée et abstraite les besoins fonctionnels et de sécurité;
(ii) implémenter des mécanismes de sécurité indépendamment du code de l'application;
(iii) définir de manière explicite les liens entre l'implémentation et la spécification.
La méthode est basée sur l'utilisation de méthodes formelles, permettant ainsi l'utilisation de techniques de vérification formelle qui assurent d'une part la cohérence et l'adéquation des politiques de sécurité par rapport aux spécifications fonctionnelles et d'autre part la cohérence de l'implémentation par rapport à la spécification.

Le projet reposera sur des méthodes et techniques existantes qui ont fait leur preuve chacune dans leur domaine particulier. Au niveau CIM, les politiques de sécurité seront décrites avec le modèle OrBAC qui permet de prendre en compte les quatre types de propriétés de sécurité. Concernant le niveau PIM, nous utiliserons UML et les méthodes formelles de type modèle qui sont bien adaptées à ce type de systèmes et possèdent un processus de raffinement formel. Au niveau du PSM, nous utiliserons une technologie web services avec un stockage des données dans des SGBD relationnels et des fichiers XML.

Les résultats attendus du projet sont alors:

- au niveau CIM : un environnement pour exprimer formellement les objectifs et les besoins de sécurité. Les besoins de sécurité seront exprimés avec OrBAC, les objectifs de sécurité avec la logique déontique.
- au niveau PIM : un environnement qui permet d'une part d'exprimer des besoins fonctionnels et de sécurité et d'autre part de vérifier leur cohérence. Cet environnement est fondé sur:
    - un enrichissement d'UML avec des concepts des modèles de sécurité qui permettent d'exprimer les besoins de sécurité spécifiés au niveau CIM.
    - la définition d'une méthode qui réalise l'intégration de notations UML et de notations formelles pour vérifier la cohérence de la spécification globale (aspects fonctionnels et sécurité) par des techniques de preuve et de test.
- au niveau PSM : la spécification d'un modèle d'implantation qui inclut un gestionnaire de vérification des politiques de sécurité s'appuyant sur les mécanismes de sécurité existants dans les technologies utilisées dans le projet et qui les coordonne;
- du PIM au PSM : deux techniques seront utilisées dans le projet. La première suit une approche classique MDA et consiste à définir un ensemble de règles de transformation. La seconde suit une approche méthode formelle et consiste à adapter leur processus de raffinement aux spécificités du domaine.
- une validation des résultats précédents sur deux études de cas du domaine médical.

Abstract

The SELKIS project aims at elaborating a development method for secure Information System (IS). The method addresses the functional and security aspects from the earliest abstraction stages of the development and combines the security mechanisms supported by data repositories and the application programs at the implementation level. The proposed approach fits a wide variety of information systems. In this project it will be experimented on medical information systems. The method must take into account the following security properties: Availability, Confidentiality, Integrity, Traceability that are crucial in this kind of IS.

The method is compliant with the MDA approach that allows an IS to be described at three abstraction levels. The first step consists in creating a Computational Independent Model (CIM) by considering various kinds of business requirements (including security requirements) collected from the IS-to-build and its environment. The second step is to elaborate a Platform Independent Model (PIM) which allows the IS-to-build to be described at an abstract level. In order to implement the PIM, it is transformed into a Platform Specific Model (PSM) that takes into account implementation issues. In the project we consider a platform implemented using a Web services technology where data are stored in relational databases and XML files.

The main goal of the project is threefold:
i) to separately and abstractly specify functional business requirements and security business requirements,
ii) to implement security mechanisms independent from the application code and
iii) to explicitly define links between the implementation and the specification.
The method is based on formal methods, enabling the use of formal verification techniques to ensure on the one hand the consistency and adequacy of security policies with respect to functional business specifications and on the other hand the consistency of the implementation with respect to the specification.

The method will take advantage of existing methods, models, and techniques coming from different research areas. At the CIM level, security policies will be described with the OrBAC model that allows the four kinds of security properties to be taken into account. At the PIM level, we will consider UML, as it is the most widely used notation in the domain of IS specification, and model-based formal methods (such as B or Z) since they have proved to be well adapted to the specification of IS and they offer a well-founded refinement process to generate implementations. At the PSM level, we will use a Web services technology with relational databases and XML files.

The intended results of the project are:

- At the CIM level : a framework to formally express security objectives and requirements. Security requirements will be expressed with OrBAC, security objectives with the deontic logic.
- At the PIM level: a framework to express and check the consistency of security and functional requirements. This framework is based on:
    - an enrichment of UML with features of security models to express security requirements defined at the CIM level.
    - the definition of a method for the integration of UML notations with formal notations to check the consistency of the global specification (functional and security elements) using proof or testing techniques.
- At the PSM level: the specification of an implementation model that includes a policy enforcement manager that takes into consideration existing security mechanisms provided by the underlying technologies used in the project and that coordinate them;
- From the PIM to the PSM: two techniques will be used in the project. The first one is compliant with the MDA approach and the result is a set of transformation rules. The second one consists in adapting the refinement process existing in formal methods to the specificities of the application domain.
- A validation of the previous results on two case studies of the healthcare domain.

Objectifs globaux, verrous scientifiques et techniques

The SELKIS project aims at elaborating a method for building secure web IS that takes into account the four ACIT facets of security at all the steps of IS development. The objectives are threefold:

i) to separately and abstractly specify functional business requirements and security business requirements,

ii) to implement security mechanisms independent from the application code,

iii) to explicitly define links between the implementation and the specification.

The method is based on formal methods, enabling the use of formal verification techniques to ensure on the one hand the consistency and adequacy of security policies with regard to functional business specifications and on the other hand the consistency of the implementation with regard to the specification.

We want to separate functional and security specifications, in order to streamline maintenance and foster sustainability. This enables one to change security policies at runtime without having to recompile the entire application. In Web systems, there are various granularity levels at which security can be specified: data attributes, atomic services (transactions) and business processes (a complex ordering of atomic services). We plan to consider these three levels.

We plan to take up the following challenges:

- Is it possible to define an abstract model that considers both the functional and security requirements of IS?
- All the existing combinations between UML and B or Z consider only functional aspects of a system, is it possible to adapt some of them to consider also security properties or is it necessary to define new integration schemes?
- Up to now, security mechanisms available at the implementation level have been separately implemented and then the global consistency is difficult to establish. Coordinating them is a real challenge.
- Is it possible to apply the proposed approach on real size IS such as those existing in healthcare networks? The challenge is to test the scalability of the approach.

Programme de travail

The method that we plan to build is compliant with the MDA approach [MDA01], composed of three steps. The first step consists in creating a Computational Independent Model (CIM) by considering various kinds of business requirements (including security requirements) collected from the IS-to-build and its environment. The second step is to elaborate a Platform Independent Model (PIM) which allows the IS-to-build to be described at an abstract level. In order to implement the PIM, it is transformed into a Platform Specific Model (PSM) that takes into account implementation issues. In the project we consider a platform implemented using a web services technology where data are stored in relational databases and XML files.

Business security requirements of a system are collected at the CIM level by means of a security policy, that consists of high-level rules, specified more precisely at the PIM level and enforced at the PSM level by security mechanisms, that define low-level functions that implement the rules of the security policy. Thus, the main goal of the project is addressed in four steps: (i) defining a method to collect security requirements; (ii) integrating the specification of security policies during the elaboration of the PIM; (iii) coordinating, at the PSM level, the security mechanisms existing in the target implementation to enforce the chosen security policy; (iv) defining sets of transformation rules from the PIM to the PSM.

The project is composed of 6 work-packages plus a coordination task:

- WP1 deals with the formal expression and analysis of security objectives and requirements,
- WP2 and WP3 deal with the PIM. WP2 is concerned by the integration of security features into UML, whereas WP3 tackles the coupling of graphical and formal models.
- WP4 is dedicated to the PSM and the security policy deployment on a Web services architecture.
- WP5 consists in defining transformation rules from an abstract model (PIM) to an implementation model (PSM).
- WP6 applies case studies on the defined method and involves all parts of the project.

The achievement of the project will provide a methodology for implementing security policies for medical records in the health care network community. This problem becomes more and more acute because of the development of the French DMP (Dossier Médical Personnel) whose aim is to store all medical data about a patient and to share them between health professionals, the SISRA platform and more generally health care networks. From a social point of view, it will provide the assurance to the patient that his medical data won't be used by unauthorized people.

Moreover, several domains like financial systems and health management systems are subject to strict regulations like Sarbane-Oxley, HIPAAA, ... Organizations and software providers must ensure that their software comply with these regulations. The use of a method such as that of the project will certainly facilitate such activities.

With regard to the diffusion of the results, we intend to publish them in national or international conferences and journals.
Extension of the MotOrBAC toolkit will be developed as plugins. MotOrBAC is already available as an open source on sourceforge.org. The translation tool from UML to Z or B developed in WP3 will be made publicly available through a Web site.