AGENCE NATIONALE DE LA RECHERCHE ANR	**Compte-rendu intermédiaire**	

Projet ANR-08-SEGI-018

SELKIS

Programme ARPEGE 2008

A IDENTIFICATION

Acronyme du projet	SELKIS
Titre du projet	Une méthode de développement de systèmes d'information médicaux sécurisés: de l'analyse des besoins à l'implémentation.
Coordinateur du projet (société/organisme)	LACL, Université Paris-Est Créteil (UPEC)
Date de début du projet Date de fin du projet	16 décembre 2008 15 décembre 2011
Site web du projet, le cas échéant	http://lacl.univ-paris12.fr/selkis/

Rédacteur de ce rapport	
Civilité, prénom, nom	Mme Régine Laleau
Téléphone	06 67 77 44 80
Adresse électronique	laleau@u-pec.fr
Date de rédaction	Août 2010
Période faisant l'objet du rapport d'activité	Février 2009/août 2010

B LIVRABLES ET JALONS

État *	**N°**	**Titre**	**Nature** (jalon, rapport, logiciel, prototype, données, …)	**Partenaires** (souligner le responsable)	**Commentaires**
Prévu 08/2010 Livré 09/2010	1.1	Formal models to express and analyze security requirements and objectives	Rapport	Telecom Bretagne	
Prévu à T0+36	1.2	Update of 1.1	Rapport	Telecom Bretagne, LIG	
Prévu 02/2010 Livré 03/2010	2.1	A UML profile for security concepts	Rapport	CEDRIC, LIG	
Prévu 02/2011	2.2	Update of 2.1	Rapport	CEDRIC, LIG, LACL	
Prévu 02/2012	2.3	Update of 2.2	Rapport	CEDRIC, LIG, LACL	
Prévu 08/2010 Livré 09/2010	3.1	Principles of the coupling between UML and formal notations	Rapport	LIG, LACL	
Prévu 02/2011	3.2	Update of 3.1 and principles of the V&V activities	Rapport	LIG, LACL	
Prévu 02/2012	3.3	Demonstration of the prototype (translator + V&V tools)	prototype	LIG, LACL	
Prévu 02/2010 Livré 03/2010	4.1	Functionalities of the policy enforcement manager	Rapport	LACL, SWID	
Prévu 02/2011	4.2	Implementation of Web services for security enforcement	prototypes	SWID, LACL	
Prévu 02/2011	5.1	Specification of the translation rules	Rapport	LACL, CEDRIC, Telecom Bretagne, SWID	
Prévu 02/2012	5.2	Definition of a set of refinement rules	Rapport	LACL, CEDRIC, Telecom Bretagne, SWID	
Prévu 02/2012	5.3	Implementation of translation plugins	prototype	Télécom Bretagne, SWID	
Prévu 02/2010 Livré 03/2010	6.1.1	Analysis of security requirements for Res@mu	Rapport	LIG, IFREMMONT	
Prévu 02/2011	6.1.2	Modelling and verification of the Res@mu model	Rapport	LIG, IFREMMONT	
Prévu 02/2012	6.1.3	Implementation of the Res@mu model	Prototypes/logiciel	LIG, IFREMMONT	
Prévu 02/2010 Livré 03/2010	6.2.1	workflow analysis and requirement specifications of the 2nd case study	Rapport	MED.e.COM, Telecom Bretagne, CHU Brest	
Prévu 08/2010 Reprévu 12/2010	6.2.2	mini-PACS deployment with basic security rules	logiciel	MED.e.COM, Telecom Bretagne, CHU Brest	Retard dans le déploiement
Prévu 02/2012	6.2.3	security tools integration in mini-PACS and upgrade at CHU	Prototypes/logiciel	MED.e.COM, Telecom Bretagne, CHU Brest	

C RAPPORT D'AVANCEMENT SUR LA PERIODE CONCERNEE

C.1 DESCRIPTION DES TRAVAUX EFFECTUES

L'objectif du WP1 est d'analyser les différentes normes qui peuvent être définies par un législateur à propos des informations qu'un système d'information peut communiquer à un agent. La démarche consiste à analyser les effets qu'un acte de communication réalisé par un système d'information peut avoir sur un agent et à analyser les effets et actions que le législateur peut choisir de permettre ou d'interdire. La technique utilisée pour faire cette analyse consiste à exprimer les notions pertinentes en logique modale. Le WP1 s'intéresse ensuite à la dérivation semi-automatique des exigences de sécurité sous forme d'une politique de sécurité. Il s'agit de partir d'une spécification Kaos du système considéré qui est expurgée des aspects fonctionnels et transformée en une spécification Kaos restreinte aux aspects de sécurité. La spécification obtenue est enrichie par les données d'une analyse de risques menée sur le système. Finalement, la dernière étape du processus consiste à dériver à partir de cette spécification Kaos transformée la politique de sécurité OrBAC (Organisation Based Access Control) correspondante. Le WP1 s'intéresse également à l'expression formelle et la mise en oeuvre d'un contrôle de sécurité *a posteriori*, une approche nécessaire lorsqu'on s'intéresse à des domaines d'application relatifs à la santé comme c'est le cas dans le cadre du projet SELKIS. L'idée est d'avoir une politique plus flexible qui ne bloque pas forcément les actions entreprises par les utilisateurs du système mais leur fait confiance tout en les responsabilisant. Un système de trace et un processus d'audit sont mis en place pour la détection des violations et le recueil des preuves. Ils sont généralement accompagnés de réactions et de sanctions éventuelles. Ces premiers résultats font l'objet du livrable L1.1. L'avancement des travaux dans le WP1 est conforme au plan initialement prévu.

Un des objectifs du WP2 est de prendre en compte l'ensemble des propriétés DICT de la sécurité en combinant une approche dirigée par les buts et un processus d'ingénierie des systèmes d'information fondé sur MDA. L'analyse des systèmes d'information permet d'affirmer que les besoins découlent des objectifs (buts) de l'organisation, des acteurs et de l'environnement dans lequel évolue le système d'information. De plus, les propriétés DICT sont très générales et indépendantes des plateformes et modèles d'implémentation. La revue de la littérature et l'analyse approfondie des besoins de sécurité nous ont mené à la conclusion que la prise en compte de l'ensemble des exigences fonctionnelles et de sécurité devait être traitée au niveau CIM (Computational Independent Model) puisqu'elle intègre notamment des aspects organisationnels fondamentaux en termes de sécurité. Nous avons donc décidé de concevoir, dans un premier temps, un méta-modèle de sécurité au niveau CIM incluant la représentation des buts fonctionnels et de sécurité, la représentation du processus de gestion supporté par le système d'information et, enfin, la représentation de l'organisation dans laquelle ce processus s'insère (acteurs, rôles, structures, etc.). Un méta-modèle PIM (Platform Independent Model) a été produit. Le travail en cours concerne notamment la définition de règles de passage du niveau CIM au niveau PIM. Ces premiers résultats font l'objet du livrable 2.1. Comme prévu, une thèse sur cette problématique a commencé. Toutefois, les contraintes opérationnelles de démarrage du projet ont entraîné un retard de calendrier de 6 mois environ. Ce retard administratif entraînera probablement un décalage dans les résultats de fin de projet. La nécessité de commencer par une modélisation au niveau CIM et le retard dans le recrutement du doctorant génèrent un décalage dans la définition du « bridge » PIM prévu entre besoins fonctionnels et besoins de sécurité.

L'objectif du WP3 est de traduire des descriptions de niveau PIM (Platform Independent Model) des applications sécurisées vers des spécifications formelles. Celles-ci pourront ensuite être animées et analysées pour vérifier et valider leurs propriétés de sécurité. La première étape de cette tâche est de proposer une traduction des modèles PIM en spécifications formelles, avec dans un premier temps la définition des principes de cette traduction et dans un deuxième temps leur mise en œuvre dans un outil. Les modèles PIM consistent d'une part en un modèle fonctionnel de l'application (diagramme de classes, enchaînement des opérations) et d'autre part en une description des règles de contrôle d'accès, suivant le méta-modèle de sécurité défini par le WP2. La traduction de ces modèles commence par la définition des règles de transformation des diagrammes du modèle fonctionnel vers un langage formel (B ou Z). Il s'agit d'une part de la traduction de diagrammes de classes en B et en Z et d'autre part, de la traduction de modèles de comportement ASTD en B. Pour la traduction des règles de contrôle d'accès, l'approche choisie consiste à définir formellement un noyau de sécurité générique, indépendant de l'application protégée et de lier ensuite ce noyau aux diverses opérations à sécuriser dans le modèle fonctionnel. Les principes de cette traduction ont été définis et expérimentés en Z. En parallèle avec la

définition de ces règles de transformation, un environnement support de permettant de configurer les transformations de modèles a été réalisé. Il permet d'appliquer sélectivement des règles de transformation différentes aux éléments du modèle (par exemple, pour traduire différemment un objet sécurisé et un objet non sécurisé). Cet environnement sera expérimenté dans l'implémentation des règles de transformation vers B. Le premier livrable (3.1), prévu à T0+18 sera livré d'ici septembre 2010. Cependant, le retard de la tâche WP2 et l'engagement tardif d'un doctorant (en juin 2009) ont retardé les phases de traduction du modèle de sécurité et de réalisation des outils associés.

Concernant le WP4, les solutions concrètes correspondant aux différents équipements logiques d'une infrastructure de sécurité (PAP – Policy Administration Point, PEP - Policy Enforcement Point, PDP – Policy Decision Point) ont été identifiées. Elles serviront à déployer une architecture complète et cohérente, de type SOA. Les travaux ont également permis d'avancer sur les outils de sécurité existants et sur la génération automatique de politiques de sécurité à destination d'équipements de sécurité. Cette génération s'appuie sur deux types d'expression haut niveau des politiques de sécurité. Le premier est réalisé en OrBAC (Organization Based Access Control) pour une déclinaison en XACML directement interprétée par un PEP. Cette première approche est intégrée dans la plateforme Protekto. La seconde méthode pour exprimer des politiques de sécurité est réalisée en EB3/ASTD avec comme objectif une implémentation BPEL. Plusieurs solutions d'implémentation sont à l'étude et feront l'objet de comparaison de performances.
Sur ce WP, l'avancement des travaux est conforme au calendrier initial.

L'objectif du WP5 est de définir un ensemble de règles de traduction des modèles de sécurité définis dans le WP3 vers des architectures de sécurité implémentées dans le WP4. Cette tâche était programmée pour démarrer 6 mois après le début du projet mais suite au retard pris dans le WP3, elle n'a vraiment démarré que depuis 6 mois. Une première étude a permis de comparer les puissances d'expression des langages EB3/ASTD et BPEL et d'en conclure que certains opérateurs des ASTD ne pouvaient pas se traduire automatiquement en BPEL. Une autre solution est maintenant envisagée. Elle consiste à partir d'un modèle Event-B obtenu à partir d'un ASTD et à utiliser le processus de raffinement formel de la méthode Event-B.

Dans le cadre du WP6.1, la première étape a consisté en l'analyse des besoins de sécurité du Res@Core (évolution du projet Res@mu). La méthode KAOS a été utilisée pour raffiner les besoins de sécurité, exprimes au niveau DICT vers une politique de contrôle d'accès exprimée par des règles RBAC. Pour ce faire, le modèle KAOS a fait l'objet d'une décomposition fonctionnelle, basée sur la structure des use cases. Les buts fonctionnels ayant accès à la cible de sécurité ont été complétés par des buts qui mettent en œuvre la politique de contrôle d'accès. Ces buts, qui sont de nature fonctionnelle font le lien entre les règles de sécurité de haut niveau et leur mise en œuvre par des règles RBAC (conformes au méta-modèle défini dans la tâche WP2 du projet Selkis). L'ensemble des résultats a permis la publication du WP6.1.1 en mars 2010.

Dans le WP6.2, le livrable 6.2.1 vise l'étude des pratiques médicales et des flux de données au sein du service d'écho-doppler (SED) au CHU de BREST en vue de définir des cas d'étude génériques à l'imagerie médicale. Ils servent de données d'entrée au WP1. Ils seront implémentés dans le WP6.2. Le travail réalisé est basé sur des visites au SED et des réunions avec les médecins et le secrétariat ainsi que le service informatique (DSIS). Les points sensibles sont notamment les interactions entre le SED et les autres services internes au CHU et les cabinets de ville, la définition de l'architecture matérielle et logicielle du service, la mise en adéquation des profils IHE « Schedule Workflow » et « Patient Information Reconciliation » sur les flux de données du SED. Le rapport final décrit 3 cas d'étude en notation UML. Il n'y a pas de dérive sur le planning initial.

Le second livrable 6.2.2 consiste à installer un serveur de résultats accessible par le WEB au SED en vue de réaliser les cas d'étude définis au WP6.2.1. A partir des résultats et des informations collectées au WP6.2.1, nous avons spécifié l'architecture matérielle et logicielle du serveur de résultats au sein du SED, notamment en termes d'interopérabilité avec les systèmes d'information (SI) du CHU. Le logiciel est installé sur notre serveur d'archivage au SED mais sans toutes les connexions avec les SI. En effet, la DSIS impose des contraintes d'installation et d'usage plus importantes qu'initialement prévues. Par exemple, l'accès à notre serveur WEB depuis l'extérieur du CHU ne sera possible qu'en 2011. Le retard prévu est de 4 mois sur le planning, soit un livrable en décembre 2010. Il n'y a pas d'impact sur les autres étapes du projet.

C.2 RESULTATS MARQUANTS (SI APPLICABLE)

C.3 REUNIONS DU CONSORTIUM (SI APPLICABLE)

Seules les réunions plénières qui ont eu lieu depuis le dernier rapport ANR (juillet 2009) sont indiquées. Plusieurs réunions internes à chaque workpackage ont également été organisées.

Date	Lieu	Partenaires présents	Thème de la réunion
27-28 janvier 2010	Rennes	CEDRIC, LACL, LIG, MED.e.COM, SWID, Telecom Bretagne	Exposés par les partenaires sur leur état d'avancement Préparation des livrables Travail intra-workpackages
28-29 avril 2010	Paris	CEDRIC, IFREMMONT, LACL, LIG, MED.e.COM, SWID, Telecom Bretagne	Discussion sur les méta-modèles de sécurité du WP2 Préparation de la revue mi-parcours ANR
5-6 juillet 2010	Paris	CEDRIC, LACL, LIG, MED.e.COM, SWID, Telecom Bretagne	Bilan et discussion sur la revue mi-parcours ANR Exposés par les partenaires sur leur état d'avancement Préparation des livrables

C.4 COMMENTAIRES LIBRES

Commentaire du coordinateur

Le projet avance bien malgré les retards pris dans certains WP par rapport aux prévisions initiales. Ces retards, hormis ceux liés à l'embauche tardive de doctorants, sont inévitables dans un projet de recherche car ils font suite à une étude approfondie du domaine et vont nous permettre de définir une méthode plus complète que celle initialement prévue.
Les échanges entre les partenaires sont très riches et plusieurs articles multipartenaires sont en cours de soumission.

Commentaire des autres partenaires

La collaboration entre les partenaires industriels du projet - Swid, MED.e.COM, CHU et IFREMMONT - est intéressante car elle nécessite d'adapter des composants de sécurité développés dans le cadre du projet à des contextes technologiques variés et innovants.

Question(s) posée(s) à l'ANR

D IMPACT DU PROJET DEPUIS LE DEBUT

D.1 INDICATEURS D'IMPACT

Nombre de publications et de communications (à détailler en D.2)

		Publications multipartenaires	Publications monopartenaires
International	Revues à comité de lecture		
	Ouvrages ou chapitres d'ouvrage		
	Communications (conférence)		6
France	Revues à comité de lecture		2
	Ouvrages ou chapitres d'ouvrage		
	Communications (conférence)		2
Actions de diffusion	Articles vulgarisation		
	Conférences vulgarisation		
	Autres	1 poster	1 poster 2 conférences invitées 2 organisations de conférences

Autres valorisations scientifiques (à détailler en D.3)

	Nombre, années et commentaires (valorisations avérées ou probables)
Brevets internationaux obtenus	
Brevet internationaux en cours d'obtention	
Brevets nationaux obtenus	
Brevet nationaux en cours d'obtention	
Licences d'exploitation (obtention / cession)	Serveur de résultats médicaux de MED.e.COM. 2009. 7 ventes Création prévue d'une forge open source à partir de Res@Core et Res@mont
Créations d'entreprises ou essaimage	
Nouveaux projets collaboratifs	
Colloques scientifiques	
Autres (préciser)	

D.2 LISTE DES PUBLICATIONS ET COMMUNICATIONS

Communications internationales avec comité de programme

W. PAN, G. COATRIEUX, J. MONTAGNER, N. CUPPENS-BOULAHIA, F. CUPPENS, C. ROUX, Comparison of some reversible watermarking methods in application to medical images, 31st IEEE International Conference of the Engineering in Medicine and Biology Society, 02-06 september 2009, Mineapolis, United States, 2009

S. PREDA, N. CUPPENS-BOULAHIA, F. CUPPENS, J. GARCIA ALFARO, L. TOUTAIN, Model-driven security policy deployment: property oriented approach. ESSoS'10 : International symposium on engineering secure software and systems , 03-04 february 2010, Pisa, Italy, 2010

PAN Wei, COATRIEUX Gouenou, CUPPENS-BOULAHIA Nora, ROUX Christian, CUPPENS Frédéric, Medical image integrity control combining digital signature and lossless watermarking. Springer, Lecture notes in computer science, 2009, vol.5939, pp. 153-162

Hanieh Azkia, Nora Cuppens-Boulahia, Frédéric Cuppens, GouenouCoatrieux, Reconciling IHE-ATNA Profile with a Posteriori Contextual Access and Usage Control Policy in Healthcare Environment, 2010 Sixth International Conference on Information Assurance and Security, pp. 197-203.

Michel Embe Jiague, Marc Frappier, Frédéric Gervais, Pierre Konopacki, Régine Laleau, Jérémy Milhau, Richard St-Denis, Model-Driven Engineering of Functional Security Policies. ICEIS 2010 12th International Conference on Enterprise Information Systems 8 - 12 June 2010, Funchal, Madeira - Portugal

Jérémy Milhau, Marc Frappier, Frederic Gervais and Régine Laleau, Systematic translation rules from ASTD to Event-B, 8th International Conference on Integrated Formal Methods, 11-14 october 2010, Nancy, France, 2010. To be published in Springer-Verlag, LNCS.

Revues nationales avec comité de lecture
A. Idani, Y. Ledru, M.-A. Labiadh. Infrastructure dirigée par les modèles pour une intégration adaptable et évolutive de UML et B. RSTI - Ingénierie des Systèmes d'Information (ISI). Volume 15 (3), Hermes-Lavoisier 2010. Numéro spécial INFORSID'09/ISI.

P. Konopacki, M. Frappier, R. Laleau. MODELISATION DE POLITIQUES DE SECURITE A L'AIDE D'UNE ALGEBRE DE PROCESSUS. RSTI - Ingénierie des Systèmes d'Information (ISI). Volume 15 (3), Hermes-Lavoisier 2010. Numéro spécial INFORSID'09/ISI.

Communications nationales avec comité de programme
A. Idani, Y. Ledru and P.-Y. Schobbens. Approche formelle pour une Ingénierie des modèles sûre. In workshop LMO/SafeModels, Mars 2009.

M.-A. Labiadh, A. Idani, Y. Ledru. Approche transformationnelle à base de méta-modèles pour l'intégration de UML et de notations formelles. Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL - 2010). Poitiers, Juin 2010. (16 pages).

Poster
Akram Idani, Mohamed Amine Labiadh and Yves Ledru. Approche orientée modèles pour une intégration efficace de B et UML, Poster présenté aux journées du GDR GPL, Pau, mars 2010

Projet ANR SELKIS : Poster présenté aux journées du GDR GPL, Pau, mars 2010

Conférences invitées

Specification and management of obligations for usage control. Frédéric Cuppens. Atelier Sec-Sy, mai 2010.

Dynamic Identity and Access Management with Protekto. Frédéric Cuppens. Journées de l'IRISATECH « La sécurité des applications Web : les enjeux de l'engineering des codes », décembre 2009.

Organisation de conférences

Du piolet à l'Internet, Congrès International de Télémédecine - 9 & 10 septembre 2010 - Courmayeur. Organisé par IFREMMONT

Co-organisation de l'atelier Sec-sy (Sécurité des Systèmes d'Information et les Environnements Collaboratifs) le 25 mai 2010 par Nora Cuppens-Boulahia.

D.3 Liste des elements de valorisation

Le serveur de résultats médicaux de MED.e.COM a été lancé sur le marché français en fin 2009. Il y a eu 7 ventes réalisées à ce jour.

Un contrat d'étude de 3 ans entre MED.e.COM et Télécom-Bretagne a été signé en août 2010. Il vise la prospection de solutions de sécurité des données d'imagerie médicale (confidentiel).

IFREMMONT signale que la modélisation issue du cas d'étude qui le concerne a été réutilisée dans le projet Res@Mont (projet Alcotra Franco-Italien) dont IFREMMONT est le chef de file pour le WP télémédical. Le projet SELKIS a été présenté à IHE France (Integrating the HealthCare Enterprise), plus particulièrement au groupe de travail IHE-F-Urgences, et au GMSIH (Groupement pour la Modernisation du Système d'Information Hospitalier) et ces travaux serviront de base à l'élaboration de profils IHE adaptés au pré hospitalier.
A terme Res@Core et Res@mont devraient déboucher sur la création d'une forge open source dédié.

D.4 Personnels recrutes en CDD (hors stagiaires)

Identification				Avant le recrutement sur le projet			Recrutement sur le projet			
Nom et prénom	Sexe H/F	Adresse email (1)	Date des dernières nouvelles	Dernier diplôme obtenu au moment du recrutement	Lieu d'études (France, UE, hors UE)	Expérience prof. antérieure (ans)	Partenaire ayant embauché la personne	Poste dans le projet (2)	Date de recrutement	Durée missions (mois) (3)
Labiadh Mohamed Amine	H	Mohamed-Amine.labiadh@imag.fr		Ingénieur en informatique (Génie Logiciel) INSAT, Tunis	Hors UE	0	UJF/LIG	Doctorant	1/6/2009	36
Embe Jiague Michel	H	Michel.Embe.Jiague@USherbrooke.ca		Maîtrise en Génie Logiciel, Université de Sherbrooke, Québec (2008)	Hors UE	0	UPEC/LACL	Doctorant	1/2/2009	36
Milhau Jérémy	H	jeremilhau@gmail.com		Ingénieur ENSIIE (2008)	France	0	UPEC/LACL	Doctorant	1/2/2009	36
Vekris Dimitris	H	dvekris@hotmail.com		Ingénieur informatique NTU Athènes (2009)	UE	0	UPEC/LACL	Doctorant	1/09/2009	36
Ben Ghorbel Meriem	F						Télécom Bretagne	Post-doc	8/6/2009	7
El Rakaiby Yehia	M						Télécom Bretagne	Doctorant	1/11/09	36
BUCUMI Jean-Sylvain	H	bujesylvain@yahoo.fr		Master recherche	France	0	CEDRIC	Doctorant	15 novembre 2009	36
Hachana Safaa	F	safahachana@gmail.com		Ingénieur en informatique (novembre 2006)	Hors UE (Tunis)	3	SWID	Ingénieur	23/01/2010	6

D.5 État financier

Nom du partenaire	Crédits consommés (en %)	Commentaire éventuel
LACL	36	Le doctorant n'a été engagé qu'à partir du 1er septembre 2009
UJF/LIG	33	Le doctorant n'a été engagé qu'à partir du 1er juin 2009.
SWID	36	Les dépenses sont moins importantes en raison de délais plus importants que prévus lors de la mise en place de la collaboration avec les équipes médicales
CEDRIC-CNAM	28,4	Le doctorant n'a été engagé qu'à partir du 15 novembre 2009.
Télécom Bretagne	48,08	
Ifremmont	37	
MED.e.COM	42	
CHU Brest	13	Peu de ressources utilisées suite au retard du WP6.2

E Annexes eventuelles