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 31 aout 2012
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
Courriel	laleau@u-pec.fr
Date de rédaction	Septembre 2011
Période faisant l'objet du rapport d'activité	août 2010/septembre 2011

B LIVRABLES ET JALONS

N°	Intitulé	Nature*	Date de fourniture			Partenaires (souligner le responsable)
			Prévue initialement	Replanifiée	Livrée	
1.1	Formal models to express and analyze security requirements and objectives	Rapport	08/10		09/10	Telecom Bretagne
1.2	Update of 1.1	Rapport	02/12			Telecom Bretagne, LIG
2.1	A UML profile for security concepts	Rapport	02/10		03/10	CEDRIC, LIG
2.2	Update of 2.1	Rapport	02/11		03/11	CEDRIC, LIG, LACL
2.3	Update of 2.2	Rapport	02/12			CEDRIC, LIG, LACL
2.3bis	Update of 2.3	Rapport	nouveau	08/12		CEDRIC, LIG, LACL
3.1	Principles of the coupling between UML and formal notations	Rapport	08/10		09/10	LIG, LACL
3.2	Update of 3.1 and principles of the V&V activities	Rapport	02/11		03/11	LIG, LACL
3.3	Update of 3.2 and principles of the V&V activities	Rapport	nouveau	02/12		LIG, LACL
3.3bis	Demonstration of the prototype (translator + V&V tools)	prototype	02/12	08/12		LIG, LACL
4.1	Functionalities of the policy enforcement manager	Rapport	02/10		03/10	LACL, SWID
4.2	Implementation of Web services for security enforcement	prototypes	02/11		03/11	SWID, LACL
4.3	Comparative study of the different SOA architectures for security	Rapport	nouveau	08/12		SWID, LACL
5.1	Specification of the translation rules	Rapport	02/11		03/11	LACL, Telecom Bretagne, SWID
5.1bis	Update of 5.1	Rapport	nouveau	08/11	11/11	LACL, Telecom Bretagne, SWID
5.2	Definition of a set of refinement rules	Rapport	02/12	08/12		LACL, Telecom Bretagne, SWID
5.3	Implementation of translation plugins	prototype	02/12			Télécom Bretagne, SWID
6.1.1	Analysis of security requirements for Res@mu	Rapport	02/10		03/10	LIG, IFREMMONT
6.1.2	Modelling and verification of the Res@mu model	Rapport	02/11	08/11	11/11	LIG, IFREMMONT
6.1.3	Implementation of the Res@mu model	Prototypes/ logiciel	02/12	08/12		LIG, IFREMMONT
6.2.1	workflow analysis and requirement specifications of the 2nd case study	Rapport	02/10		03/10	MED.e.COM, Telecom

N°	Intitulé	Nature*	Date de fourniture			Partenaires (souligner le responsable)
			Prévue initialement	Replanifiée	Livrée	
						Bretagne, CHU Brest
6.2.2	mini-PACS deployment with basic security rules	logiciel	08/10	08/11	07/11	MED.e.COM, Telecom Bretagne, CHU Brest
6.2.3	security tools integration in mini-PACS and upgrade at CHU	Prototypes/ logiciel	02/12	08/12		MED.e.COM, Telecom Bretagne, CHU Brest

** jalon, rapport, logiciel, prototype, données, …*

C RAPPORT D'AVANCEMENT

C.1 OBJECTIFS INITIAUX DU PROJET

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.

C.2 TRAVAUX EFFECTUÉS ET RÉSULTATS ATTEINTS SUR LA PÉRIODE CONCERNÉE

Les travaux réalisés durant cette période dans le cadre du WP1 concernent la modélisation en logique modale des propriétés de confidentialité et d'intégrité des systèmes d'information en termes d'agents institutionnels, humains et logiciels. Concernant les travaux sur le contrôle d'accès et d'usage, une formalisation en logique descriptive des données contrôlées est en cours. Les éléments nécessaires au contrôle d'accès et d'usage lorsque les données sont de type « imagerie médicale » ont été formalisés en logique classique et sous forme de règles ECA et tatoués dans les images. Une spécification du module de confiance assurant les contrôles d'usage et la traçabilité à été faite. L'avancement des travaux dans le WP1 est conforme au plan initialement prévu.

Concernant le WP2, dans le livrable 2.2, ont été mentionnées les améliorations apportées au méta-modèle CIM suite à son application au système d'information pré-hospitalier de Ifremmont. Nous avions aussi produit une nouvelle version des profils UML pour le niveau PIM (celle relative à la description des fonctionnalités et celle associée à la description de la structure statique du système d'information) ainsi qu'une nouvelle version du processus de transformation d'une instance du méta-modèle CIM en une instance du méta-modèle des cas d'utilisation ainsi qu'un ensemble de règles de transformation.
Durant la période écoulée, nous avons travaillé sur la transformation d'une instance du méta-modèle CIM en une instance du méta-modèle PIM décrivant la structure statique d'un système d'information sécurisé. Cette instance est un diagramme des classes décrivant les aspects organisationnels d'un système d'information sécurisé au niveau PIM. Nous avons à cet effet produit quelques règles de transformation.
De plus, nous nous sommes intéressés au cours de cette période écoulée, suite à un stage de Master 2, à la déduction semi-automatique des exigences de sécurité à partir d'une analyse des risques. Nous avons produit pour cela : (1) deux ontologies alignées (l'une représentant les risques potentiels encourus par les entreprises et l'autre représentant les exigences de sécurité potentielles) et (2) un processus de dérivation semi-automatique basé sur les deux

ontologies. Ce travail vient compléter les résultats obtenus dans le livrable 1.1.

L'objectif du WP3 est de traduire des descriptions de niveau PIM (Platform Independent Model) des applications sécurisées vers des spécifications formelles. Les travaux menés au cours des douze derniers mois se sont attachés à traduire des descriptions UML conformes à la partie PIM du métamodèle produit par la tâche WP2 vers des descriptions formelles écrites en B ou en Z. Concernant la traduction en Z, des règles de traduction ont été proposées dans le cadre de la thèse de Nafees Qamar. Elles permettent d'obtenir une spécification qui intègre les aspects fonctionnels et sécuritaires d'un modèle UML étendu avec un profil sécuritaire (proche de notre métamodèle et de SecureUML). La spécification formelle peut ensuite être analysée, notamment par simulation. Ces analyses ont permis de trouver des trous de sécurité sur des exemples déjà publiés indépendamment. Concernant la traduction en B, elle fait l'objet d'une collaboration entre le LIG et le LACL, avec notamment un séjour de M.A. Labiadh dans l'équipe du LACL. Ces collaborations ont permis de définir comment combiner trois facettes de la spécification : aspects fonctionnels, propriétés invariantes de sécurité, propriétés dynamiques de sécurité. Ces règles font actuellement l'objet d'une implémentation dans un environnement de multi-traduction développé au LIG.

Concernant le WP4, une architecture complète et cohérente d'une infrastructure de sécurité (PAP – Policy Administration Point, PEP - Policy Enforcement Point, PDP – Policy Decision Point), de type SOA, a été déployée autour du prototype CLIPPER de Medecom. D'autres implémentations SOA en BPEL permettant d'exprimer des politiques de sécurité réalisée en EB3/ASTD sont en cours de développement et feront l'objet de comparaison de performances, dans le cadre de la thèse de Michel Embe-Jiague. Nous avons également défini un méta-modèle d'un PEM (Policy Enforcement Manager) au niveau PSM qui nous permettra de comparer les différents types d'architectures SOA développées dans le projet.

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. Deux types d'étude ont été menées. Une première étude consite à traduire une spécification de contrôle d'accès exprimée en ASTD en un ensemble de processus BPEL, elle est décrite dans la thèse de Michel Embe-Jiague. Une autre solution, décrite dans la thèse de Jérémy Milhau, consiste à partir d'un modèle B obtenu à partir d'un ASTD et à utiliser le processus de raffinement formel de la méthode B.

Dans le cadre de la tâche WP6.1, l'analyse des besoins a été menée pendant les premiers mois avec la méthode KAOS. L'effort est actuellement porté sur la traduction d'un sous-ensemble de l'étude de cas dans le langage B. Cette activité a pris du retard suite aux retards pris par le WP3 dans la réalisation des outils.
D'autres travaux concernant les tâches WP6.1 et WP6.2 sont décrits dans la partie C.5 de ce document.

C.3 DIFFICULTÉS RENCONTRÉES ET SOLUTIONS

Nous avons obtenu une prolongation du projet de 6 mois, jusqu'à fin aout 2012. Comme détaillé dans la lettre de demande de prolongation, plusieurs raisons ont justifié cette demande. La première est d'ordre technique et concerne le WP6.2.2. Il était prévu à T0+18 et n'a été déployé qu'à T0+29. Ce retard est essentiellement dû à des lourdeurs administratives et au nombre élevé d'interlocuteurs au CHU de Brest. Ceci entraîne automatiquement un retard dans la livraison du livrable 6.2.3. Ce livrable consiste à compléter le serveur sécurisé avec de nouvelles fonctionnalités de sécurité. Initialement, un délai de 18 mois était prévu entre les deux livrables. Cependant, le prototype étant déjà bien avancé chez Medecom, Telecom Bretagne et SWID, il pourra être déployé au CHU de Brest à T0+42, soit en août 2012.

La deuxième raison est d'ordre scientifique. Il concerne le WP 2, "Integration of security features into UML". Comme nous l'avons déjà mentionné dans le compte-rendu intermédiaire à T0+18, il a fallu concevoir et valider un méta-modèle CIM pour représenter, au niveau CIM et à un grain très fin, les liens entre les exigences fonctionnelles et les exigences non fonctionnelles (notamment la sécurité). Ce méta-modèle CIM est décrit dans le livrable L2.1. Il a été modifié comme le décrit le livrable L2.2 après avoir été appliqué sur l'étude de cas Ifremmont du projet. Ce retard du WP 2 a eu logiquement un impact sur les WPs 3, 5 et 6.1. Mais la prolongation de 6 mois du projet nous permettra de mener à bien les objectifs que nous avions fixés.

C.4 FAITS ET RÉSULTATS MARQUANTS

Les résultats marquants du CEDRIC, LACL, LIG et Télécom Bretagne ont fait l'objet de communications dans des revues et des conférences internationales.
L'application Medecom a été sécurisée de façon efficace tout en rendant dynamique les politiques de sécurité qui la gouvernent.

N. Lammari (CEDRIC) et D.G. Rosado (University of Castilla-La Mancha) ont organisé le 21 juin 2011 WISSE'11-First International Workshop on Information System Security Engineering. Ce workshop a eu lieu en conjonction

avec la conférence CAiSE'11, Londres, UK.
Une seconde édition de ce workshop aura lieu en juin 2012.

C.5 TRAVAUX SPÉCIFIQUES AUX ENTREPRISES (LE CAS ÉCHÉANT)

Entreprise	MED.e.COM SARL
Rédacteur (nom + adresse mél)	Michel COZIC / michel.cozic@medecom.fr

Livrable 6.2.2 :
L'installation et la mise en production du MiniPACS (CLIPPER) au CHU, prévue fin 2010, est effective depuis juillet 2011, avec la collaboration du service informatique du CHU. Le logiciel intègre la messagerie sécurisée avec APICRYPT et permet la transmission du compte rendu d'examen aux prescripteurs conformément au décret Confidentialité de mai 2007.

Livrable 6.2.3 :
Nous avons participé à la réalisation par SWID d'un prototype de CLIPPER qui s'interface au logiciel MotOrBAC par des Web Services. Nous avons depuis amélioré la politique de sécurité et la conformité au modèle ORBAC de CLIPPER en tenant compte de nos retours d'expérience.
Les contrôles d'intégrité et d'authenticité par le tatouage d'images sont disponibles par une API de Telecom Bretagne Brest, validée par Medecom. Cette première version limite les usages, notamment en termes de performances. De nombreux échanges avec Telecom Bretagne apportent des solutions à tester dans une seconde phase. L'interface de l'API avec CLIPPER est prévue à compter de novembre 2011 avec en particulier la réalisation d'un plugin pour le navigateur Firefox.
L'authentification forte des utilisateurs par la carte CPS est à l'étude, à partir du cahier des charges de l'ASIP Santé et des solutions commerciales sur le marché.
La conformité au profil IHE ATNA est en cours de réalisation, suite à la demande de Telecom Bretagne Rennes pour l'étude du contrôle d'accès à postériori.

Entreprise	SWID
Rédacteur (nom + adresse mél)	Stéphane Morucci / stephane.morucci@swid.fr

Dans le cadre de la tâche WP6.2, Swid a porté sur Windows et a intégré ses différentes solutions logicielles (serveurs d'authentification, d'autorisation et ses agents) au sein du progiciel Medecom. Le fonctionnel du système ainsi intégré a été validé. L'authentification et l'autorisation sont maintenant déléguées à des serveurs spécialisés. Concernant le contrôle d'accès, toutes les exigences de sécurité fournies par Medecom ont été formalisées dans le modèle propriétaire Swid (niveau CIM) puis traduites en RDF et XACML, la version XACML servant à piloter le PEP Swid, interrogé par l'agent intégré au sein du progiciel Medecom.
Concernant Iffremont, les exigences de sécurité ont là aussi été formalisées dans un modèle propriétaire haut-niveau puis traduites en XACML et RDF. La technologie AOP (Programmation par Aspect) a été utilisée pour injecter , par configuration, une solution de délégation d'autorisation pilotée par une politique CIM/PIM traduite automatiquement par les outils mis en place par le projet Selkis. Le principal avantage de cette technologie AOP concerne la faible adhérence résultante entre les contrôles de sécurité et le fonctionnel de l'application initiale. Le déploiement réel sur le progiciel Iffremont est prévu pour la fin d'année 2011. Cette action n'avait pas été prévue initialement dans le projet.

Entreprise	Ifremmont
Rédacteur (nom + adresse mél)	Dr Pascal ZELLNER / pascal@ifremmont.com

La plateforme ResaCore intègrera le moteur de sécurité issu du projet SELKIS et des travaux du LIG. Nous attendons la publication du WP6.1.3 pour implémenter ce moteur de règles au sein du noyau de la plateforme. Le branchement sera effectué au travers de Spring Security® et des annotations AOP. Une première version du noyau a été confié à SWID afin d'effectuer des tests d'utilisation du serveur SWID de sécurisation.

L'architecture ResaCore dédiée à la télémédecine sera bien publiée en 2012 au travers d'une forge Open Source, les perspectives d'utilisations sont nombreuses. La version V1 sera publiée avec notre propre moteur de sécurité. Nous attendrons une version ultérieure pour intégrer les résultats SELKIS qui au delà de la revue de la modélisation a déjà permis d'améliorer la construction de l'ontologie du projet.

Entreprise	CHRU BREST
Rédacteur (nom + adresse mél)	Luc BRESSOLLETTE / luc.bressollette@chu-brest.fr

Livrable 6.2.2 :
Le CHU de Brest, par ses équipes techniques, a participé à l'installation et à la mise en production du MiniPACS de la société MEDECOM au sein du service d'écho-doppler, soit :

- réalisation de l'infrastructure réseau TCP/IP,
- configuration de la worklist DICOM entre les échographes et le SIH AGFA,
- l'achat et la préparation du serveur RAID5 suivant les recommandations de MEDECOM,
- l'interopérabilité des échographes avec le MiniPACS

- mise en place de la télémaintenance du serveur par la société MEDECOM

D'autre part, le CHU de BREST vient de recruter un ingénieur en CDD.

C.6 RÉUNIONS DU CONSORTIUM (PROJETS COLLABORATIFS)

Seules les réunions plénières qui ont eu lieu depuis le dernier rapport ANR (septembre 2010) sont indiquées. Plusieurs réunions internes à chaque workpackage ont également été organisées.

Date	Lieu	Partenaires présents	Thème de la réunion
13-14 janvier 2011	Chamonix	CEDRIC, IFREMMONT, LACL, LIG, MED.e.COM, SWID, Telecom Bretagne	Exposés par les partenaires sur leur état d'avancement Préparation des livrables Travail intra-workpackages Préparation de la demande de prolongation du projet
5-6 juillet 2011	Paris	CEDRIC, IFREMMONT, LACL, LIG, MED.e.COM, CHU Brest, SWID, Telecom Bretagne	Exposés par les partenaires sur leur état d'avancement Préparation des livrables Bilan du workshop WISSE@CAISE 2011 Travail intra-workpackages

C.7 COMMENTAIRES LIBRES

Commentaires du coordinateur

Le projet avance bien malgré les retards pris dans certains WP par rapport aux prévisions initiales. Le fait d'avoir obtenu une prolongation du projet permettra de combler ces retards et d'obtenir des résultats très intéressants. Plusieurs thèses viennent ou vont se terminer avant la fin du projet, ce qui est déjà en soi un résultat scientifique important du projet. Nous allons continuer à développer les échanges entre partenaires, en particulier pour la rédaction d'articles multipartenaires.

Commentaires des autres partenaires

Concernant l'UJF/LIG, l'accent a été mis pendant les douze derniers mois sur la traduction du modèle PIM dans la tâche WP3. Cela a donné lieu à plusieurs résultats et à une forte activité de publication. La collaboration avec le LACL a également porté des fruits, notamment en matière de publications. Dans les prochains mois, l'effort portera sur les contributions de l'UJF/LIG dans la tâche WP6.1 et l'application des résultats obtenus sur cette étude de cas.
La collaboration entre les partenaires industriels du projet, notamment entre Swid, MED.e.COM et IFREMMONT, se poursuit de manière très fructueuse et aboutira à des implémentations concrètes à la fin du projet.

Question(s) posée(s) à l'ANR

D VALORISATION ET IMPACT DU PROJET DEPUIS LE DEBUT

Nous détaillons ici les éléments qui concernent la période Septembre 2010 – Septembre 2011. Les informations précédant cette période sont disponibles sur le site du projet.

D.1 PUBLICATIONS ET COMMUNICATIONS

Liste des publications multipartenaires (résultant d'un travail mené en commun)		
International	**Revues à comité de lecture**	1. Référence 1 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.
	Communications (conférence)	1. Références 3 et 4 2.
France	**Revues à comité de lecture**	1. 2.
	Ouvrages ou chapitres	1.

	d'ouvrage	2.
	Communications (conférence)	1. 2.
Actions de diffusion	**Articles de vulgarisation**	1. 2.
	Conférences de vulgarisation	1. 2.
	Autres	1. 2.

Liste des publications monopartenaires (impliquant un seul partenaire)		
International	**Revues à comité de lecture**	1. Référence 2 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.
	Communications (conférence)	1. Références 5 à 18
France	**Revues à comité de lecture**	1. 2.
	Ouvrages ou chapitres d'ouvrage	1. 2.
	Communications (conférence)	1. Référence 19 2.
Actions de diffusion	**Articles de vulgarisation**	1. 2.
	Conférences de vulgarisation	16. Le projet Res@Core qui intègre la méthodologie SELKIS sera présenté à la conférence M Health http://www.mhealth2011.com/conference-j2.html 17.
	Autres	2. 3.

Revues internationales avec comité de lecture

1. Jérémy Milhau, Akram Idani, Regine Laleau, Mohamed Amine Labiadh, Yves Ledru and Marc Frappier. "Combining UML, ASTD and B for the Formal Specification of an Access Control Filter", Innovations in Systems and Software Engineering, Springer, pages: 1-11, Octobre 2011, online available : http://www.springerlink.com/content/f9wu85p14361p76l/
2. Michel Embe Jiague, Marc Frappier, Frédéric Gervais, Régine Laleau and Richard St-Denis. "Enforcing ASTD Access-Control Policies with WS-BPEL Processes in SOA Environments" International Journal of Systems and Service-Oriented Engineering, IJSSOE 2(2): 37-59, 2011

Communications internationales avec comité de programme

3. Yves Ledru, Akram Idani, J. Milhau, Muhammad Nafees Qamar, Régine Laleau, Jean-Luc Richier, Mohamed-Amine Labiadh. "Taking into account functional models in the validation of IS security policies." International Workshop on Information Systems Security Engineering (WISSE'11), Advanced Information Systems Engineering Workshops - CAiSE 2011 International Workshops, 83:592--606, Lecture Notes in Business Information Processing, London, UK, jun 2011.
4. Jérémy Milhau, Akram Idani, Regine Laleau, Mohamed Amine Labiadh, Yves Ledru and Marc Frappier. "Combining UML and B for the Formal Specification of an Access Control Filter" Fourth IEEE International workshop UML and Formal Methods, Limerick, june 2011
5. Lammari N., Bucumi J., Akoka J., Comyn-Wattiau I. «A Conceptual Meta-Model for Secured Information Systems». Int. Work. on Soft. Eng. for Secure Sys. (SESS'11) in conjonction with Int. Conf. on Soft. Eng. (ICSE'11).
6. Lammari N., Bucumi J., Akoka J., Comyn-Wattiau I. «Un modèle CIM pour les systèmes d'information sécurisés». The 15th IBIMA (International Business Information Management Association) conference on Knowledge Management and Innovation: A Business Competitive Edge Perspective (IBIMA'10), Cairo, Egypt, 2010.
7. Yves Ledru, Muhammad Nafees Qamar, Akram Idani, Jean-Luc Richier, Mohamed-Amine Labiadh."Validation of security policies by the animation of Z specifications." Proceedings of the 16th ACM symposium on Access control models and technologies, (SACMAT'11), 155-164, Innsbruck, Austria, 2011.
8. Yves Ledru, Jean-Luc Richier, Akram Idani, Mohamed-Amine Labiadh. "From KAOS to RBAC: a Case Study in Designing Access Control Rules from a Requirements Analysis." Proceedings of the 6th Conf. on Network Architectures and Information Systems Security (SAR-SSI 2011), 157-164, La Rochelle, France, 2011.
9. Muhammad Nafees Qamar, Yves Ledru, Akram Idani. "Evaluating RBAC Supported Techniques and Their Validation and Verification." Fifth International Workshop on Secure Software Engineering (SecSE'11) in conjunction with 6th IEEE International Conference on Availability, Reliability and Security (ARES'11), Vienna, Austria, aug 2011. Muhammad Nafees Qamar, Yves Ledru, Akram Idani. "Validation of Security-Design Models

using Z." Proceedings of the 13th International Conference on Formal Engineering Methods (ICFEM 2011), 6991:259-274, LNCS, Durham, United Kingdom, oct 2011.
10. M. Embe Jiague, M. Frappier, F. Gervais, P. Konopacki, R. Laleau, J. Milhau, R. St-Denis: A four-concern-oriented secure IS development approach. In 8th International Joint Conference on e-Business and Telecommunications (ICETE 2011), Seville, Spain, 18-21 July. INSTICC Press, volume SECRYPT 2011, pp. 464-471, 2011.
11. M. E. Jiague, M. Frappier, F. Gervais, R. Laleau, R. St-Denis "A Metamodel of an Access-Control Policy Enforcement Manager", 4th Canada-France MITACS Workshop on Foundations & Practice of Security, May 2011, Paris, France, Springer-Verlag, LNCS 6888, à paraitre
12. J. Milhau, R. Laleau, M. Frappier "A Metamodel for Static and Dynamic Access Control Policies", 4th Canada-France MITACS Workshop on Foundations & Practice of Security, May 2011, Paris, France, Springer-Verlag, LNCS 6888, à paraître
13. Michel Embe Jiague, Marc Frappier, Frederic Gervais, Regine Laleau, and Richard St-Denis "From ASTD Access Control Policies to WS-BPEL Processes Deployed in a SOA Environment", WISS 2011, LNCS 6724, Springer-Verlag Berlin Heidelberg, pp. 126-141, 2011.
14. Pan W, G. Coatrieux, J. Montagner, N. Cuppens, F. Cuppens, C. Roux. Reversible Watermarking based on Invariant Image Classification and Dynamical Error Histogram Shifting. Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 2011.
15. Pan, W., G. Coatrieux, N. Cuppens, F. Cuppens, et C. Roux. An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform. Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC): 4740-4743, 2010.
16. Pan, W., G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, et C. Roux. Watermarking to Enforce Medical Image Access and Usage Control Policy. Sixth International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), pp. 251-260, 2010.
17. Mariem Graa, Nora Cuppens-Boulahia, Fabien Autrel (Telecom Bretagne), Hanieh Azkia, Frederic Cuppens, Gouenou Coatrieux, Ana Cavalli, Amel Mammar. Using Requirements Engineering in an Automatic Security Policy Derivation Process, 4th International Workshop on Autonomous and Spontaneous Security (SETOP); Leuven, 2010.
18. D. Bouslimi, G. Coatrieux, C. Roux, "A Joint Watermarking/Encryption Algorithm for Verifying Medical Image Integrity and authenticity in Both Encrypted and Spatial Domains", IEEE EMBC'11, Boston, USA.

Communications nationales avec comité de programme

19. D. Bouslimi, G. Coatrieux, M. Cozic, Ch. Roux, « Tatouage-chiffrement conjoint pour le contrôle de la fiabilité des images médicales » RITS, Rennes, France, 2011.

D.2 AUTRES ÉLÉMENTS DE VALORISATION

Liste des éléments. Préciser les titres, années et commentaires	
Brevets internationaux obtenus	1. 2.
Brevet internationaux en cours d'obtention	20. 21.
Brevets nationaux obtenus	1. 2.
Brevet nationaux en cours d'obtention	1. 2.
Licences d'exploitation (obtention / cession)	1. 13 licences de CLIPPER vendues dont 2 à l'export depuis le début du projet
Créations d'entreprises ou essaimage	1. 2.
Nouveaux projets collaboratifs	1. Sous-traitance avec Télécom Bretagne sur 3 ans à compter d'octobre 2010
Colloques scientifiques	1. WISSE'11-First International Workshop on Information System Security Engineering. Ce workshop a eu lieu en conjonction avec la conférence CAiSE'11, Londres, UK, 21 juin 2011. Il a été organisé par N. Lammari (CEDRIC) et D.G. Rosado (University of Castilla-La Mancha) Une seconde édition de ce workshop aura lieu en juin 2012.
Autres (préciser)	1. 2.

D.3 PÔLES DE COMPÉTITIVITÉ (PROJET LABELLISÉS)

Le projet SELKIS n'est pas labellisé par un pôle de compétitivité.

D.4 PERSONNELS RECRUTÉS 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
Wang François	M						Télécom Bretagne	Ingénieur	1/07/2009	3
Talbi Mehdi	M						Télécom Bretagne	Ingénieur	1/11/2010	6
Dalel Bouslimi	F						Télécom Bretagne	Doctorant	1/10/2010	12
Wei Pan	M						Télécom Bretagne	Doctorant	1/10/2010	12
Hui Huang	F						Télécom Bretagne	Doctorant	1/02/2010	4
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
Philippe TIGREAT	H	philippe.tigreat@gmail.com		Ingénieur en traitement du signal et de l'information Telecom Bretagne à Brest ()	France	0	CHU de BREST	Ingénieur	12/09/2011	10

D.5 ÉTAT FINANCIER

Nom du partenaire	Crédits consommés (en %)	Commentaire éventuel
LACL	72	Le doctorant n'a été engagé qu'à partir du 1er septembre 2009
UJF/LIG	71	Le doctorant n'a été engagé qu'à partir du 1er juin 2009.
SWID	72	nous n'avons pas trouvé de stagiaires ni de CDD pertinents pour le projet. Avec l'accord de l'ANR, les crédits alloués pour le personnel non-permanent seront reportés pour du personnel permanent.

CEDRIC-CNAM	60,52	Le doctorant n'a été engagé qu'à partir du 15 novembre 2009.
Télécom Bretagne	85.59	
Ifremmont	100	
MED.e.COM	69	
CHU Brest	19	L'nstallation du serveur a été réalisée par du personnel permanent. Le reste du crédit va servir à financer l'ingénieur recruté en septembre 2011, ainsi qu'un stagiaire.

E ANNEXES EVENTUELLES