

Rapport d'activité n°3

A. Identification

Programme – année	ARA – SSIA - 2005
Projet (acronyme)	Cops
Nom du coordonnateur du projet et affiliation (société/organisme - laboratoire ou entité de rattachement)	Philippe Balbiani Institut de recherche en informatique de Toulouse (UMR 5505)
Référence convention ou décision	Décision n° ANR-05-SSIA-0007-01
Projet : date de début – date de fin	Composition de politiques et de services 24 janvier 2006 - 23 janvier 2009
Période faisant l'objet du rapport d'activité (date début – date fin)	1er juillet 2007 - 31 mars 2008
Rédacteur de ce rapport : nom	Philippe Balbiani
téléphone	05.61.55.60.91
adresse électronique	Philippe.Balbiani@irit.fr
Date du rapport	1er juin 2008

B. Rappel des tâches allouées par partenaire pour l'ensemble du projet (partir du planning généralement fourni dans le projet. Ce document est à remplir par le coordonnateur du projet à partir des informations fournies par chacun des partenaires)

Ce tableau (à compléter) décrit les principales tâches du projet qui ont été définies lors de son démarrage

Tâches du projet	Partenaires concernés par la tâche (2)		2006		2007	2008	Commentaires
			Semestre 1 (1)	Semestre 2 (1)			
Langages pour l'expression de politiques de sécurité	P1, P2, P3	Prévue/Nouvelle	P	P	P	P	
		Réalisée/Abandonnée		R	R	R	
Combinaison de politiques de sécurité et de services électroniques	P1, P2, P3	Prévue/Nouvelle	P	P	P	P	
		Réalisée/Abandonnée		R	R	R	
Algorithmes pour la composition de services électroniques	P1, P2, P3	Prévue/Nouvelle	P	P	P	P	
		Réalisée/Abandonnée		R	R	R	

(1) P=Prévue, N=Nouvelle, R=Réalisée, A=Abandonnée (dans ce dernier cas, justifier obligatoirement avec un commentaire)

(2) Partenaires concernés : ceux-ci sont à expliciter dans un tableau (cf. ci-dessous)

Partenaire P1	Institut de recherche en informatique de Toulouse / Toulouse / Equipe Lilac	Philippe Balbiani
Partenaire P2	Laboratoire lorrain de recherche en informatique et ses applications et	Michael Rusinowitch

	Laboratoire d'informatique de l'université de Franche-Comté / Nancy et Besançon / Projet Cassis	
Partenaire P3	Laboratoire d'informatique fondamentale de Marseille / Marseille / Equipe Move	Denis Lugiez

Eléments qualitatifs

C. Description des travaux effectués pour la période concernée et conformité de l'avancement aux prévisions (15 à 50 lignes maximum suivant le nombre de partenaires)

(1) Langages pour l'expression de politiques de sécurité : Notre travail consiste à définir, pour les services Web, une variante du contrôle d'accès basé sur les rôles (RBAC) avec laquelle les services Web exprimeront leurs politiques de sécurité. La variante que nous proposons est basée sur les notions de requête et de certificat. Chaque service définit sa politique sous la forme de règles statiques qui viennent dire quels certificats doivent accompagner les requêtes auxquelles il accepte de répondre. Des règles dynamiques régissent la façon dont les réponses aux requêtes acceptées seront faites. Cette variante que nous proposons fait l'objet d'un rapport de recherche [1].

(2) Combinaison de politiques de sécurité et de services électroniques : Nos travaux consistent à introduire dans le modèle standard des protocoles cryptographiques un symbole associatif-commutatif ainsi que des symboles unaires permettant de représenter des arbres XML. Il est réalisé en collaboration entre les 3 partenaires. Nos recherches portent plus précisément sur la validation de protocoles cryptographiques permettant de prendre en compte des contraintes plus larges et d'exprimer des politiques de sécurité. Les résultats obtenus sur les techniques de vérification de ces protocoles sont de deux ordres: un résultat de combinaison général qui donne un cadre permettant d'exprimer les protocoles sous forme de workflow avec des règles non déterministes et qui donne une technique de combinaison de procédures de décision ; un résultat montrant comment on peut enrichir la description des services ou protocoles en incluant des contraintes positives d'inclusion. Les difficultés techniques pour la méthode de combinaison sont particulièrement complexes mais ont pu être surmontées alors que l'extension naturelle aux contraintes d'inclusion négatives n'a pas débouché. Afin de mieux comprendre le problème, un travail d'étude de la résolution de contraintes sous-termes en présence de contraintes d'appartenance à un langage régulier a débuté. Une autre piste explorée a été de généraliser le résultat de décision de l'absence d'attaque sur les protocoles dans le cas d'un ensemble d'hypothèses infini mais régulier. La question est de savoir si un résultat sur les clés atomiques peut être généralisé aux clés quelconques.

(3) Algorithmes pour la composition de services électroniques : Le problème de la composition de services consiste à combiner un ensemble de services afin de répondre à la requête d'un client. Les services sont des éléments logiciels indépendants qui peuvent être composés en vue de faire collaborer entre elles des applications distribuées. La composition des services étudie les situations où les demandes des clients ne peuvent être satisfaites qu'en combinant les services disponibles de manière appropriée. Dans le modèle sur lequel nous travaillons, les services Web sont modélisés comme des machines à états finis (automates) avec échanges de messages. L'alphabet de ces automates sont les actions et les messages échangés. Le problème auquel nous nous intéressons est le suivant: étant donné un ensemble de services Web et un service abstrait (le service but) décrivant le résultat que l'on souhaite obtenir, comment composer cet ensemble de services de telle sorte que le service but soit satisfait ?

D. Résultats obtenus pour la période concernée, dégager notamment les faits marquants (15 à 50 lignes maximum) *Décrire les résultats obtenus et préciser éventuellement les livrables déjà réalisés en interne au projet.*

(1) Langages pour l'expression de politiques de sécurité : Le contrôle d'accès basé sur les rôles (RBAC) est l'objet de plusieurs langages de politique. Cela est dû à son expressivité en termes de gestion des problèmes de contrôle d'accès dans des systèmes complexes. Cependant, bien que très expressifs, la plupart des langages de haut-niveau manquent d'un aspect dynamique dans l'expression et l'évaluation des règles de contrôle d'accès. Ainsi, dans cet article on propose un langage de haut niveau qui prend en compte les propriétés de RBAC et ses extensions mais présente aussi un aspect dynamique dans l'expression des règles de contrôle d'accès. L'idée générale est de considérer le système de contrôle d'accès comme un contexte de décision et un ensemble statique de règles Datalog. Le contexte de décision est un ensemble de permissions, tel que chacune des permissions est obtenue à partir des règles Datalog statiques et des permissions déjà existantes dans le contexte de décision. L'aspect dynamique provient du fait que chaque action a une conséquence, ainsi le système de contrôle d'accès évolue d'un contexte de décision à un autre selon les actions exécutées par l'utilisateur. Dans l'article [4] on présente le langage, des exemples d'expressions des propriétés de RBAC et une analyse de complexité pour des problèmes de décision concernant le contrôle d'accès dans notre langage.

(2) Combinaison de politiques de sécurité et de services électroniques : Les services Web envoient et reçoivent des messages codés en XML. En conformité avec le standard de sécurité des services Web, quelques parties de ces messages échangés sont hachés, chiffrés ou signés. Nous avons introduit un modèle qui décrit formellement les protocoles de communication que nous utilisons dans les services Web, leurs propriétés de sécurité ainsi que leurs possibles failles, appelées attaques de réécriture. A la différence des autres modèles de protocoles (dans l'analyse symbolique), les nôtres peuvent gérer des échanges non déterministes de messages ainsi qu'une séquence non ordonnée de nœuds XML. Ensuite, pour détecter les attaques, nous considérons les services comme des combinaisons des opérateurs de multi-ensembles et des opérateurs cryptographiques et nous avons à résoudre les spécifiques problèmes de satisfiabilité dans la théorie combinée. Par une extension non triviale des techniques de combinaison, nous obtenons une procédure de décision pour le problème d'insécurité des services Web où les messages sont construits en utilisant les fonctions de chiffrement, les schémas de signature ainsi que d'autres primitives cryptographiques. Cette technique de combinaison nous permet d'avoir un algorithme qui décide le problème de l'insécurité d'une façon modulaire et ceci en réduisant les problèmes associés de résolution de contraintes en des problèmes de résolution de contraintes dans des théories plus simples. Les techniques connues d'analyse des protocoles considèrent la classe des protocoles où certaine partie d'information prévue dans un message du protocole doit apparaître à une position fixe. Pourtant, cette hypothèse est trop restrictive pour modéliser les services Web où les messages sont des documents XML semi-structurés et où des informations doivent être extraites à partir des nœuds apparaissant dans des positions flexibles. Par conséquent, nous avons étendu le modèle de Dolev-Yao par un prédicat de sous-termes qui nous permet d'exprimer l'extraction des données par une correspondance des sous-termes. Ceci nous permet aussi de détecter les attaques de réécritures spécifiques aux services Web. Ces résultats ont donné lieu aux publications [5] et [6].

(3) Algorithmes pour la composition de services électroniques : Pour composer entre eux les services, on essaie de coordonner les échanges de messages. Cependant, si la coordination ne satisfait pas le service but, on essaie alors de générer un nouveau service, appelé médiateur. Le rôle de ce dernier est d'essayer de générer les flux de messages manquants à la composition, i.e. lorsqu'un service indispensable à la composition attend un message pour s'exécuter et qu'il ne le reçoit pas, alors le médiateur va tenter de générer ce message. Ainsi, la coordination est constituée de plusieurs étapes. La première consiste à filtrer la communauté de services Web afin de créer des groupes, appelés clusters. Chaque cluster contient un ensemble de services Web capables d'échanger des messages. Le but du filtrage est de cerner les services capables de communiquer. Une fois les clusters construits, on procède à la coordination des services Web via le produit cartésien des services du cluster éligible. Un cluster est dit éligible si l'ensemble de son alphabet couvre celui du service but. La coordination résultant du produit cartésien peut disposer des traces d'exécution pour lesquelles la composition échoue. Un cas d'échec intervient lorsque dans une

trace un message ne peut pas être reçu, i.e., le service correspondant reste bloqué en attente du message. Pour éviter un tel blocage, le filtrage proposé consiste à masquer toutes les transitions ainsi que les traces sous-jacentes pour lesquelles au moins un message est attendu mais pas envoyé auparavant. Quant aux transitions pour lesquelles les contraintes liées à l'envoi et à la réception du message ne sont pas compatibles, on supprime définitivement les traces correspondantes. Une fois obtenue la composition filtrée, i.e., elle ne contient pas de cas de blocage, on peut alors procéder à la vérification de la satisfaction du service but par la coordination. Si la composition ne satisfait pas le service but, alors on essaie de générer un nouveau service, appelé médiateur qui tente de rendre les traces bloquantes exécutables. Ainsi, dans le modèle que nous proposons, le rôle du médiateur est de générer les messages manquants. Ce modèle, ainsi que des algorithmes décrivant la construction d'une composition et du médiateur, a fait l'objet de la rédaction de plusieurs articles [1,2,8,9].

Nos travaux portent également sur la prise en compte des contraintes temporelles dans le processus de composition. Dans le cadre de l'analyse de la compatibilité et de la substitution dynamique des services Web, les conversations sont modélisées par les machines à états finis où les états correspondent aux états du service et les transitions correspondent aux échanges de messages (messages reçus ou émis). Les contraintes temporelles d'activations permettent de déclencher une transition automatiquement et ce après l'écoulement d'un certain délai. Nous nous intéressons au problème de compatibilité en utilisant une modélisation à base de WSTTS (Web Services Timed Transition Systems). Nos premiers résultats sur le sujet ont été présentés au workshop WWV'2007 [8]. Dans ce papier, nous nous focalisons sur différents aspects pertinents pour l'analyse de la compatibilité: messages échangés, données échangées, contraintes relatives aux données et contraintes temporelles. Nous y étudions trois classes de compatibilité: compatibilité absolue, compatibilité éventuelle et incompatibilité absolue.

E. Difficultés rencontrées et solutions de remplacement envisagées (15 à 50 lignes maximum) *ex : impasse technique, abandon d'un partenaire ou d'un sous traitant, maîtrise des délais, maîtrise des budgets. Faut-il revoir le contenu du projet ? Faut-il revoir le calendrier du projet ?*

(1) Langages pour l'expression de politiques de sécurité : Aucune.

(2) Combinaison de politiques de sécurité et de services électroniques : Aucune.

(3) Algorithmes pour la composition de services électroniques : Aucune.

F. Livrables externes réalisés (15 à 50 lignes maximum)

Pour les articles et communications écrites, préciser s'il s'agit d'articles dans des revues à comité de lecture / d'ouvrages ou chapitres d'ouvrage / d'articles dans d'autres revues / de communications dans des colloques ou des congrès / de dépôt de brevet... Référencer selon les normes habituelles. Mentionner également s'ils peuvent ou non faire l'objet de communications externes par l'ANR et son unité support

Indiquer, Le cas échéant, les thèses démarrées, en cours et/ou soutenues en relation directe avec le projet :

Préciser le titre, date de soutenance (prévue ou réelle), soutien financier, devenir des étudiants pour les thèses soutenues

Publications :

[1] P. Balbiani, F. Cheikh, G. Feuillade. Composition of interactive Web services based on controller synthesis, in: 2nd International Workshop on Web Service Composition and Adaptation (WSCA-2008), à paraître.

[2] P. Balbiani, F. Cheikh, G. Feuillade. Composition of Web services: algorithms and complexity, in: 1st International Workshop on Interaction and Concurrency Experience (ICE-2008), à paraître.

[3] P. Balbiani, F. Cheikh, G. Feuillade, P.-C. Heam, O. Kouchnarenko, J. Voinot. Composition of

Web services with static constraints, en préparation.

[4] P. Balbiani, Y. Chevalier, M. El Hourri. A logical approach to role-based access control in a distributed environment, in: Proceedings of the 13th International Conference on Artificial Intelligence: Methodology, Systems, Applications (AIMSA-2008), à paraître.

[5] Y. Chevalier, D. Lugiez, M. Rusinowitch. Towards an Automatic Analysis of Web Service Security, in: Proceedings of the 6th International Symposium on Frontiers of Combining Systems (FroCoS-2007), F. Wolter (editor), Lecture Notes in Artificial Intelligence, Springer, September 2007, vol. 4720, p. 133-147.

[6] Y. Chevalier, D. Lugiez, M. Rusinowitch. Verifying Cryptographic Protocols with Subterms Constraints, in: Logic for Programming, Artificial Intelligence, and Reasoning, 14th International Conference (LPAR-2007), N. Dershowitz, A. Voronkov (editors), Lecture Notes in Artificial Intelligence, Springer, October 2007, vol. 4790, p. 181-195.

[7] Y. Chevalier, A. Mekki, M. Rusinowitch. Automatic Composition of Services with Security Policies, in: 2nd International Workshop on Web Service Composition and Adaptation (WSCA-2008), à paraître.

[8] N. Guermouche, O. Perrin, C. Ringeissen. Timed Specification For Web Services Compatibility Analysis, in: Proc. of 3rd International Workshop on Automated Specification and Verification of Web Systems (WWV-2007).

[9] N. Guermouche, O. Perrin, C. Ringeissen. A Mediator Based Approach For Services Composition, 2007, Research report Inria.

[10] P.-C. Heam, O. Kouchnarenko, J. Voinot. Towards Formalizing QoS of Web Services with Weighted Automata, 2007, Research report Inria.

Thèses démarrées (depuis le début du projet) :

[1] Fahima Cheikh. Modèles et algorithmes pour la composition de services. Doctorat préparé à l'université Paul Sabatier depuis septembre 2005. Soutenance prévue en juillet 2008. Financement sur contrat.

[2] Marwa El Hourri. Langages de haut niveau pour l'expression de politiques d'échanges de messages entre services. Doctorat préparé à l'université Paul Sabatier depuis juin 2006. Soutenance prévue en mai 2009. Financement sur contrat.

[3] Nawel Guermouche. Vérification de la politique de sécurité des services. Doctorat préparé à l'université Henri Poincaré depuis octobre 2006. Soutenance prévue en septembre 2009. Bourse Inria/Région.

[4] Mounira Kourjeh. Analyse de la sécurité des protocoles avec primitives cryptographiques imparfaites. Doctorat préparé à l'université Paul Sabatier depuis janvier 2006. Soutenance prévue en décembre 2008. Financement sur contrat.

[5] Stéphane Martin. Vérification de Web services. Doctorat préparé à l'université de Provence depuis septembre 2007. Soutenance prévue en juillet 2010. Bourse MNERT.

[6] Anis Mekki. Politiques d'échange de certificats dans les services électroniques. Doctorat préparé à l'université Henri Poincaré depuis octobre 2007. Soutenance prévue en juillet 2010. Financement sur contrat.

[7] Vincent Prêtre. Génération automatique de tests à partir de modèle formel pour les applications de type web services. Doctorat préparé à l'université de Franche-Comté depuis octobre 2005. Soutenance prévue en septembre 2008. Financement sur contrat.

[8] Pablo Seban. Vérification de politiques de sécurité exprimées en logique non classiques. Doctorat préparé à l'université Paul Sabatier depuis septembre 2007. Soutenance prévue en juillet 2010. Bourse MNERT.

[9] Jérôme Voinot. Approximations et model-checking pour la sécurité de systèmes distribués. Doctorat préparé à l'université de Franche-Comté depuis octobre 2006. Soutenance prévue en septembre 2009. Bourse MNERT.

G. Autres commentaires

Eléments quantitatifs

H. Liste des réunions/séminaires/colloques organisés durant la période et des missions à l'étranger

(préciser la date, le lieu, l'objet, le nombre des participants)

Réunions : Les activités du projet Cops sont décrites à l'adresse suivante www.irit.fr/COPS/Accueil.htm.

La première réunion a eu lieu au laboratoire d'informatique fondamentale de Marseille du 16 au 17 mars 2006. La seconde réunion a eu lieu à l'institut de recherche en informatique de Toulouse du 5 au 6 octobre 2006. La troisième réunion a eu lieu au laboratoire lorrain de recherche en informatique et ses applications du 29 au 30 mars 2007. La quatrième réunion a eu lieu au laboratoire d'informatique de l'université de Franche-Comté du 7 au 8 février 2008.

Des rencontres et des visites ponctuelles ont eu lieu : visite de Philippe Balbiani au LIFC du 19 au 20 février 2007, visite de Philippe Balbiani et Fahima Cheikh au Loria du 22 au 23 février 2007, visite de Fahima Cheikh au Loria du 27 au 28 mars 2007. De nombreuses rencontres ont eu lieu entre Yannick Chevalier, Denis Lugiez et Michael Rusinowitch pour la préparation des références [5] et [6].

I. Par rubrique et par partenaire, établir la consommation des dépenses financées par l'ANR, depuis le démarrage du projet.

Partenaire	Fonct. (Keuros)	Equipement (<i>préciser nature</i>)	Equip. (Keuros)
P1	26,1 Keuros	Aucun	0 Keuros
P2	17,1 Keuros	Ordinateurs	3 Keuros
P3	1,0 Keuros	Ordinateurs	4 Keuros

J. Le cas échéant, préciser les travaux réalisés par les partenaires étrangers associés au projet sans aide de l'ANR

Dans le projet initial, Cédric Fournet et Andrew Gordon (Microsoft Research, Cambridge) avait été associés au projet. Ils n'ont jamais répondu favorablement à nos invitations à participer à nos réunions.

K. Liste des personnels recrutés en CDD par des établissements publics dans le cadre du projet sur l'aide allouée par l'ANR

Nom	Prénom	Qualifications	Date de recrutement	Durée du contrat (en mois)
...				
...				

Indiquer leur devenir postérieur à leur participation au projet : intégration comme chercheur, enseignant-chercheur, ingénieur, emploi dans le privé, chômeur, etc....

Aucun personnel n'a été recruté en CDD dans le cadre du projet.

L. Le cas échéant, indiquer les différents types d'aides complémentaires obtenues grâce à ce projet.

(Il peut s'agir de ressources financières, ressources humaines, allocations de recherche,...)

Le partenaire P2 bénéficie d'un financement par le plan Etat - région Lorraine dans le cadre de l'action QSL COWS ("Contraintes pour la composition de services web") du thème "Qualité et sûreté des logiciels et systèmes informatiques". Cette action est coordonnée par Olivier Perrin (Loria) et Laurent Vigneron (Loria). Elle a démarré en 2006 et durera 2 années.

Les partenaires P1 et P2 sont également partenaires du projet européen (FP7, ICT Security, 2008-2010) AVANTSSAR (Automated Validation of Trust and Security of Service-Oriented Architectures) qui vient d'être sélectionné et accepté. Les autres partenaires de ce projet sont : Université de Vérone, IBM (Zurich), Siemens (Munich), SAP (Sophia-Antipolis), ETH Zurich, Université de Gênes, IDEALX (Paris) et Institut e-Austria Timisoara (Timisoara).

M. Le cas échéant, modalités d'utilisation du complément de financement « pôles de compétitivité » (15 lignes maximum)

Rappel : ceci ne s'applique pas aux entreprises, mais seulement aux laboratoires publics et autres structures non soumises à l'encadrement communautaire des aides d'Etat à la R&D. Le complément de financement est destiné à couvrir des frais supplémentaires liés à la participation aux activités du pôle : ingénierie de projets partenariaux publics-privés, recherche de partenaires ; valorisation de la recherche ; relations inter-pôles et internationales...

Nous ne bénéficions d'aucun complément de ce type.

N. CADRE RESERVE AU COORDONNATEUR DU PROJET (15 à 50 lignes maximum)

Commentaire général sur l'état d'avancement du projet, les interactions entre les différents partenaires, les efforts particuliers en matière d'interdisciplinarité, l'ouverture internationale, etc.

Dans le cadre de la tâche **Algorithmes pour la composition de services électroniques**, Philippe Balbiani (Irit), Fahima Cheikh (Irit), Nawel Guermouche (Loria), Olivier Perrin (Loria) et Christophe Ringeissen (Loria) ont travaillé ensemble sur la difficulté intrinsèque du problème de la composition des services électroniques qui intègrent les notions de temps et de confiance. Une réunion entre ces personnes a eu lieu à Nancy en février 2007, une autre réunion a eu lieu à Nancy en mars 2007.

Yannick Chevalier (Irit), Denis Lugiez (Lif) et Michael Rusinowitch (Loria) ont travaillé ensemble à la réalisation de la tâche **Combinaison de politiques de sécurité et de services électroniques**. Ils ont préparé ensemble deux rapports de recherche [5,6].

Dans le cadre de la tâche **Algorithmes pour la composition de services électroniques**, Philippe Balbiani (Irit), Fahima Cheikh (Irit), Pierre-Cyril Heam (LIFC), Olga Kouchnarenko (LIFC) et Jérôme Voinot (LIFC) ont travaillé ensemble sur la difficulté intrinsèque du problème de la composition des services électroniques qui intègrent les notions de coût et de confiance. Une réunion entre ces personnes a eu lieu à Besançon en février 2007. Ils préparent ensemble le rapport de recherche [3].

CADRE RESERVE A l'USAR

Nom du coordinateur scientifique de l'USAR :

Date :

Glossaire

Livrable : tout composant matérialisant le résultat de la prestation de réalisation. Toute production émise par le titulaire au cours du projet : document, courrier revêtant un caractère officiel , module de code logiciel, dossiers de tests, application intégrée, objet, dispositif...

Livrable interne : réalisé au sein du programme et non communiqué à l'extérieur du programme.

Livrable externe : élément diffusé ou livré hors de la communauté du projet de recherche..

Faits marquants : élément non nécessairement quantifiable mais significatif pour le projet.