

	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 : Depuis sa conception en 1992, le modèle RBAC (role-based access control) est devenu la référence incontournable des systèmes de contrôle d'accès. Il a été étendu dans de nombreuses directions de façon indépendante : RBAC avec délégation, RBAC avec obligation, etc. Ces extensions sont inadaptées pour les grandes organisations (comme les services) dans lesquelles, par exemple, les concepts de délégation ou d'obligation peuvent avoir différents sens et doivent, en conséquence, être implémentés de différentes façons. Notre travail consiste à définir, pour les services Web, une variante de RBAC avec laquelle les services Web exprimeront leurs politiques de sécurité.

(2) Combinaison de politiques de sécurité et de services électroniques : Nous avons travaillé sur les politiques de sécurité au niveau des messages, et leur prise en compte pour la recherche d'attaques sur des services sécurisés. Ces travaux ont consisté d'abord à introduire, dans le modèle standard des protocoles, un symbole associatif-commutatif ainsi que des symboles unaires permettant de représenter des arbres XML.

(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.

Nous avons défini un modèle formel à base d'automates pondérés permettant de représenter des services et leurs compositions à partir de fichiers de description (extension des standards WSDL et BPEL). Nous avons proposé cette extension dans le but de démontrer l'applicabilité de l'approche proposée). Nous avons considéré ensuite les notions de substitutivité et de compatibilité entre services pour pouvoir décider si un service peut être remplacé par un autre et si des services peuvent être composés entre eux pour répondre à une demande spécifique (problème de synthèse). Pour le problème de la substitutivité, nous avons développé un prototype permettant d'automatiser la vérification des conditions établies pour certaines classes d'automates pouvant être rencontrés dans le cadre de la modélisation. Ce prototype est capable de tenir compte de contraintes temporelles sur les communications entre services (timeout).

Dans le cadre d'une collaboration entre l'Irit et le LIFC, nous avons étudié le problème de la composition qui tient compte de la confiance que les services ont envers les autres et qui influe sur les certificats qu'ils échangent.

Enfin, nous proposons une méthodologie pour la composition automatique de services Web. Dans cette approche, la composition est basée sur la coordination de services grâce à des échanges de messages. Nous utilisons des automates conversationnels, ou les transitions sont conditionnées par les données échangées et produites. D'autre part nous travaillons à une modélisation par des contraintes dans laquelle l'idée est d'instancier un schéma de composition pré-établi, en fonction de

la requête d'un client. L'instantiation est obtenue de façon incrémentale, en propageant les contraintes attachées aux services. La principale difficulté de ce problème concerne l'étude de la complexité des algorithmes que nous avons développés, qu'il s'agisse des algorithmes de construction du produit cartésien des services, ou de la gestion des contraintes à chaque étape de la composition.

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 : Notre travail consiste à définir, pour les services Web, une variante de RBAC avec laquelle les services Web exprimeront leurs politiques de sécurité. Comme pour le langage Cassandra, nous proposons un langage dans lequel RBAC peut être plongé et dans lequel on peut coder les notions de délégation et d'obligation. Notre langage est basé sur l'hypothèse que le mécanisme de contrôle d'accès peut être séparé en une partie statique et une partie dynamique. Dans l'article [1], nous avons étudié notre langage du point de vue de sa complexité algorithmique et du point de vue de son expressivité. Nous avons également discuté de son implémentation en XACML.

(2) Combinaison de politiques de sécurité et de services électroniques : Les contraintes imposées par les politiques de sécurité sur les messages XML sont différentes de celles rencontrées dans l'étude de protocoles cryptographiques, dans le sens où les messages acceptables sont définis par des expressions XPath au lieu d'avoir une structure fixée. Nous avons abordé la prise en compte de ces contraintes en traitant dans un premier temps le cas de contraintes sous-termes, exprimant par exemple qu'une signature doit être présente dans le message. Actuellement, nous étendons ces premiers résultats à des contraintes qui permettent de modéliser les schémas XML, mais aussi de caractériser le résultat d'expressions XPath sur un document. Voir les références [2] et [3].

(3) Algorithmes pour la composition de services électroniques : Nous avons obtenu des résultats de décidabilité sur la substitution de services au sein d'une composition en tenant compte de critères de QoS ainsi que des résultats de décidabilité sur la compatibilité de services Web. Également, nous avons obtenu un modèle de coordination basé sur la construction d'un produit d'automates et la création d'un médiateur pour engendrer les messages manquants. Voir les références [6] et [7].

Nous avons également étudié la complexité du problème consistant à décider si une composition de services répond précisément à la requête d'un client. Nous avons déterminé des bornes inférieures et supérieures de complexité pour différentes abstractions des services et pour différentes méthodes de comparaison entre services composés et requête du client. Ces travaux ont été publiés dans l'article. Voir la référence [4].

Nous avons aussi étudié le problème consistant à fabriquer un service médiateur qui a pour objectif de dialoguer avec les services existants et avec le client afin de satisfaire la requête de ce dernier. Nous avons adapté pour cela des algorithmes issus de la théorie du contrôle des systèmes à événements discrets. En effet, le service médiateur joue le rôle d'un contrôleur pour l'ensemble des services existants et la requête du client constitue la spécification (l'objectif du problème de contrôle associé). Nous avons, dans un premier temps, identifié les cas pour lesquels le problème est décidable. Dans un deuxième temps, nous avons adapté les algorithmes de synthèse de contrôleur au cas particulier de la composition de services. Voir la référence [5].

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, Y. Chevalier, Marwa El Hourri. A logical approach to role-based access control in a distributed environment. Rapport Irit.

[2] Y. Chevalier, D. Lugiez, M. Rusinowitch. Towards an automatic analysis of Web service security. In B. Konev, F. Wolter (éditeurs) : *Frontiers of Combining Systems*. Springer (2007) 133-147.

[3] Y. Chevalier, D. Lugiez, M. Rusinowitch. Verifying Cryptographic Protocols with Subterm Constraints. Rapport Irit.

[4] P. Balbiani, F. Cheikh, G. Feuillade. Considérations relatives à la décidabilité et à la complexité du problème de la composition des services. In J. Lang, Y. Lespérance, D. Sadek, N. Maudet (éditeurs) : *Modèles formels de l'interaction*. Annales du Lamsade 8 (2007) 261-268.

[5] P. Balbiani, F. Cheikh, G. Feuillade. Composition of interactive Web services based on controller synthesis. Rapport Irit.

[6] N. Guermouche, O. Perrin, C. Ringeissen. A methodology for Web services automatic composition. Rapport Inria.

[7] E. Monfroy, O. Perrin, C. Ringeissen. Modeling Web services composition with constraints. Rapport Inria.

[8] P. Balbiani, F. Cheikh. Computational analysis of interacting Web services: a logical approach. Rapport Irit.

[9] P.-C. Heam, O. Kouchnarenko, J. Voinot. How to handle QoS aspects in Web services substitutivity verification. In 16th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE 2007), 18-20 June 2007, Paris, France.

[10] P.-C. Heam, O. Kouchnarenko, J. Voinot. Towards formalizing QoS of Web services with weighted automata. Rapport 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. Aucun soutien financier.

[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. Bourse du bureau Moyen-Orient de l'Agence universitaire de la francophonie.

[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. Bourse de la Fondation Hariri.

[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] 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.

[7] 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.

[8] 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. Les participants étaient Philippe Balbiani (Irit), Fahima Cheikh (Irit), Véronique Cortier (Loria), Yannick Chevalier (Irit), Nawel Guermouche (Loria), Marwa El Houry (Irit), Olga Kouchnarenko (LIFC), Mounira Kourjeh (Irit), Denis Lugiez (Lif), Enrica Nicolini (Loria), Olivier Perrin (Loria), Vincent Prêtre (LIFC), Silvio Ranise (Loria), Christophe Ringeissen (Loria), Michael Rusinowitch (Loria), Mathieu Turuani (Loria), Laurent Vigneron (Loria), Daniele Zucchelli (Loria).

La quatrième réunion aura lieu au laboratoire d'informatique de l'université de Franche-Comté du 22 au 23 novembre 2007.

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, rencontres entre Yannick Chevalier, Denis Lugiez et Michael Rusinowitch pour la préparation des références [2] et [3].

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	23,4 Keuros	Aucun	0 Keuros
P2	10,8 Keuros	Aucun	0 Keuros
P3	0,9 Keuros	Aucun	0 Keuros

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

Cédric Fournet et Andrew Gordon (Microsoft, Cambridge) sont associés de façon informelle au projet. Ils n'ont pas encore pu cette année 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.

Avant et après la réunion de Nancy (mars 2007), les collaborations évoquées dans le rapport semestriel se sont approfondies. En particulier :

1. 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.
2. 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.
3. 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.

Les questions que nous avons prévu d'aborder au commencement du projet trouvent peu à peu des réponses ainsi que l'attestent les publications référencées ci-dessus. Certaines de ces publications sont communes à plusieurs partenaires du projet. Au niveau du problème de la composition de services, par exemple, la réponse apportée dans la référence [5] a bénéficié, lors de son élaboration, des discussions qui ont eu lieu entre Philippe Balbiani (Irit), Fahima Cheikh (Irit), Nawel Guermouche (Loria), Pierre-Cyril Heam (LIFC), Olga Kouchnarenko (LIFC), Olivier Perrin (Loria), Christophe Ringeissen (Loria) et Jérôme Voinot (LIFC) lors des visites évoquées plus haut.

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.