OFFRE D'ALLOCATION DE THESE

ECOLE DOCTORALE
SCIENCES EXACTES ET LEURS APPLICATIONS
ED 211

SUJET DE THESE

TITRE : Contrôle d'usage dans les architectures orientées services

RESUME :

Les architectures orientées services (SOA en anglais) sont de plus en plus utilisées pour concevoir les systèmes d'information des entreprises. Que ce soit en interne au sein de l'entreprise ou en externe chez des prestataires de services, une telle organisation des moyens matériels et logiciels améliore, entre autres, leur réutilisabilité et leur interopérabilité.

Ces architectures introduisent néanmoins de nouvelles vulnérabilités et donc de nouveaux risques quant à la sécurité de l'information. Certaines technologies permettent actuellement de chiffrer les échanges, d'authentifier les clients et les fournisseurs de services, etc...

Le sujet de recherche proposé dans cette thèse aborde le problème de la sécurité de tels systèmes d'information sous l'angle du contrôle d'usage : il s'agit de surveiller comment le client utilise les différents services. Il nous faut pour cela définir un modèle d'interactions, un modèle de politiques de sécurité et un modèle de supervision (approche gestion des risques) adaptés aux architectures SOA, ceci en tenant compte des aspects juridiques liés aux moyens mis en œuvre.

Mots clés: contrôle d'usage, services, SOA, IDM, gestion de risques

CONDITIONS D'EXERCICE

Laboratoire : LIUPPA (EA n°3000)

Site web : http://liuppa.univ-pau.fr/live/

Directeur de thèse : Manuel Munier & Philippe Aniorté (équipe MOVIES)

Lieu : Mont de Marsan

Date début : septembre 2012 **durée :** 3 ans

Employeur : UPPA

Salaire mensuel net : environ 1684€/mois brut (soit environ 1370€/mois net)

Savoir-faire du laboratoire : logiciel, modélisation, visualisation, sécurité, interfaces homme-machine, systèmes d'information et réseaux

MISSION - ACTIVITÉS PRINCIPALES

Le contexte scientifique

Les architectures orientées services (SOA pour Service Oriented Architectures) telles que les services Web, le cloud computing,... se développent de plus en plus dans les systèmes d'information des entreprises. D'un point de vue technologique, ces concepts sont actuellement bien maîtrisés : langages de programmation, architecture client/serveur, normalisation des formats d'échanges,... Les préoccupations se posent dorénavant plutôt en termes de sécurité de l'information selon une approche de gestion des risques. Ces SOA tendent effectivement à rendre les systèmes d'information dépendants les uns des autres. Que ce soit au sein d'une même entreprise ou entre des organisations différentes, cette inter-dépendance des SI introduit bien évidemment de nouvelles vulnérabilités et donc, à fortiori, de nouveaux risques pour la sécurité des informations : indisponibilité des services, calculs erronés suite à l'obtention de « fausses » informations, diffusion de données incorrectes (cf. notion de responsabilité, aspects législatifs, image de marque de l'entreprise,...), utilisation non autorisée de services, mauvaises utilisation des services,... Cette liste n'est bien évidemment pas exhaustive !

Des solutions ont été développées pour répondre à certains besoins : authentification des fournisseurs de services, intégrité des données reçues, chiffrement des données échangées, authentification du client (cf. notion de transaction ou de session). Des études ont été réalisées et des préconisations ont été données pour le développement des services (sécurité côté serveur). Nous estimons que ces aspects sécuritaires ne sont toutefois pas suffisants et ne permettent pas de prendre en compte tous les risques liés à l'utilisation de tels services dans les SI actuels.

Les objectifs

Ce sujet de thèse concerne l'étude, le développement et la mise en œuvre de contrôle d'usage au sein des SOA (modèle, mécanismes, méthode). Des outils de contrôle d'accès existent déjà sur certaines architectures : « tel client a l'autorisation de se connecter à tel fournisseur de service ». Le niveau de granularité peut (éventuellement) permettre de préciser quels sont les services autorisés sur un fournisseur donné. Le contrôle d'usage permet quant à lui d'avoir une meilleure expressivité dans les politiques de sécurité en introduisant par exemple des concepts tels que les obligations, les règles contextuelles,... Les chercheurs en sécurité informatique du site montois possèdent déjà une expérience reconnue sur cette problématique du contrôle d'usage, notamment au travers de l'ANR FLUOR. Ces travaux, initiés dans le contexte de la gestion des droits numériques pour les documents d'entreprise (E-DRM pour Enterprise Digital Right Management), font actuellement l'objet d'une première adaptation au domaine du cloud (cf. publication TSIS'2012) et des services web (stage master 2 recherche en 2012).

Les résultats attendus

Outre les aspects technologiques incontournables, l'objectif de ce sujet de thèse est la définition d'un modèle de politique de sécurité adapté aux SOA d'une manière générale. L'idée étant que le modèle développé fournisse également un certain nombre « d'indicateurs » que nous pourrions réutiliser dans nos travaux de recherche sur les gestion des risques dans les SI faisant appel à des SOA, et notamment pour le développement d'un SMSI adapté. Des travaux sur ce thème « gestion des risques » ont déjà débuté dans le cadre de la thèse de Vincent Lalanne dans le contexte des SOA. Ceux-ci concernent plus précisément la démarche et la définition d'une méthode de gestion des risques. En effet, actuellement, une des préoccupations majeures de la sécurité informatique est liée aux aspects juridiques : collecte d'informations nécessaires

à la politique de sécurité (métadonnées), traitements automatiques, traçabilité (notions de preuve et de responsabilité). Nos collaborations entamées depuis plus d'un an avec, entre autres, nos collègues juristes de l'UPPA illustrent d'ailleurs les enjeux de cette problématique et l'impact envisagé sur le milieu socio-économique.

En matière de modélisation, les travaux décrits s'inscriront dans une démarche IDM (Ingénierie Dirigée par les Modèles) dont les avantages sont maintenant bien établis, tant dans le milieu académique que le milieu industriel, à savoir le niveau de formalisation, et en conséquence la possibilité de réaliser des opérations automatiques sur les modèles (transformation, fusion,...). L'objectif est de s'appuyer sur les résultats déjà obtenus en la matière, notamment en termes de métamodèles, pour les adapter et les étendre dans le but de :

- considérer plus généralement la gestion des risques, domaine plus large que celui actuellement étudié,
- cibler les systèmes basés SOA qui prennent une ampleur considérable.

Les collaborations de recherche

Juristes de l'UPPA pour la prise en compte des aspects législatifs liés aux méthodes et mécanismes mis en œuvre.

COMPÉTENCES REQUISES

Il est bien évidemment souhaitable que le candidat bénéficie déjà d'une certaine expérience en programmation orientée objet (Java, IDL,...) et en programmation réseau (RMI, CORBA, servlets, web services,...).

Une expérience supplémentaire en systèmes d'information, politiques de sécurité, gestion des risques ainsi qu'en systèmes & réseaux serait également appréciable.

CRITÈRES D'ÉVALUATION DE LA CANDIDATURE

- Autonomie, curiosité, esprit d'initiative
- Maîtrise de la langue française
- Maîtrise de l'anglais scientifique et technique

CONSTITUTION DU DOSSIER DE CANDIDATURE

- CV détaillé
- Lettre de motivation
- Lettres de recommandation (si possible)

CONTACT

manuel.munier@univ-pau.fr