Projet

MUNIER Manuel

(informatique – LIUPPA)

CONTEXTE

Les paradigmes orientées service ont considérablement changé la façon de concevoir les applications et l'organisation des entreprises. Tant l'approche SOA[1] que le Cloud ont permis l'émergence de nouveaux modèles basés sur des collaborations dynamiques. Du point de vue des utilisateurs finaux, les services offrent un accès simplifié aux fonctionnalités et aux données. Quant aux organisations, la délégation de certains processus métier représente une opportunité de générer des avantages concurrentiels en réduisant les coûts, en augmentant la visibilité sur le marché et en exploitant l'expertise de leurs partenaires en offrant à ses clients des produits et des services avec de la valeur ajoutée.

Malgré les attraits des technologies basées sur les services, la perte de contrôle sur les ressources échangées est un inconvénient bien connu qui freine leur large adoption. Essentiellement, au sein des organisations différents types des règles sont associés aux ressources afin de garantir qu'elles soient correctement utilisées. De telles règles sont associées à n'importe quelle condition visant à prévenir d'éventuels dommages organisationnels, dont nous pouvons citer les conditions assurant la prévention de la perte de réputation ou la garantie de la conformité avec une norme juridique. Cependant, à partir du moment où la ressource sort du périmètre de l'organisation, il n'y a plus aucun moyen de savoir si la ressource est utilisée en respectant les règles établies. Les conséquences d'une telle perte de contrôle sur l'utilisation ne sont pas négligeables puisque la façon dont les ressources partagées sont utilisées peut affecter l'organisation en entraînant des pénalités, la perte de clients ou des poursuites. Les impacts de ces dommages justifient la nécessité d'avoir des méthodes visant à contrôler l'utilisation des ressources partagées lors d'une prestation de services. Dans ce scénario, le défi est de garantir que le partenaire externe se comporte comme prévu lorsque la ressource est dans son domaine et et que les intérêts de chaque organisation doivent être préservés.

Dans nos travaux nous avons proposé que la prestation de services soit régie par un contrat de service. Ce contrat diffère de SLA[2] traditionnels de plusieurs façons:

- Il augmente l'expressivité des garanties de service SLA, traditionnellement basées sur la sécurité et la performance, avec des termes contractuels représentant les exigences opérationnelles sur l'utilisation prévue des ressources.
- Il est basé sur une sémantique formelle qui évite des erreurs d'interprétation des clauses contractuelles grâce à une compréhension commune de leur signification.
- La conformité avec les exigences de l'entreprise en matière d'usage des ressources est déduite de la connaissance disponible recueillie au cours de l'exécution du contrat.

Notre méthode de contrôlabilité est basée sur deux éléments. Le premier a trait à la modélisation des politiques, et la second consiste en un processus qui opère avec ces politiques. En ce qui concerne la modélisation, deux modèles complémentaires sont proposés. Un premier pour formaliser la sémantique d'un contrat de service, y compris un vocabulaire de contrôlabilité. Un second pour définir les politiques de contrôlabilité, utilisant le modèle sémantique pour donner une signification claire au comportement attendu des parties. Au cours du processus, un journal qui contient la connaissance disponible sur le comportement des parties contractuelles est utilisé pour vérifier la conformité et évaluer le comportement des partenaires. Les contrats sont créés en OWL pour être lisibles par la machine et les règles des politiques sont écrites en XML.

Cette méthode, couplée au raisonnement basé sur la connaissance, offre de nouvelles perspectives quant aux techniques d'Intelligence Artificielle appliquée aux services web. D'autre part, ces travaux ouvrent des perspectives de travaux futurs, tels que la négociation de la politique contractuelle pour les contrats multipartites.

1 SOA : Service Oriented Architecture
2 SLA : Service Level Agreement

Problématique

Nos travaux de recherche ont abouti à la définition d'un outil technologique permettant de formaliser les politiques de sécurité (via des contrats) et d'évaluer la conformité du comportement des acteurs par rapport à ces politiques (via les logs et le processus de contrôle).

Idées :

Une des perspectives à approfondir maintenant consiste à consolider ces travaux par une étude sur le volet juridique :

- Que peut-on / que doit-on faire apparaître comme règles de sécurité dans les politiques spécifiées dans les contrats ?
- Quels éléments de preuve (métadonnées) peut-on exiger ? Quelles contraintes pour leur journalisation dans les logs ?
- Sous quelles conditions, de quelle manière et jusqu'à quel point peut-on exploiter les données des logs pour engager la responsabilité (ou pas) d'un acteur ?
- Si l'on reste sur une architecture non fédérée où les contrats sont définis entre deux acteurs et sont (à priori) indépendants les uns des autres, quid de la chaîne de responsabilités en cas de sous-traitance ?

Objectifs :

De mon point de vue, une collaboration entre juristes et informaticiens sur ce thème devraient permettre :

- d'identifier les besoins / les attentes de chaque discipline vis-à-vis de l'autre
- d'étudier les solutions actuellement proposées par les outils informatiques / juridiques existants
- de proposer des pistes pour combler les manques actuels

Références Bilbiographiques

- **Thèse Elena Jaramillo** – « *A Semantic Contract Model and Knowledge-driven Process for Supporting Controllability in Service-oriented Approaches* » – encadrement P. Aniorté, M. Munier (soutenue le 12/12/2016)
- **INFORSID 2016** – « *Service Contracts: Beyond Trust in Service Oriented Architectures* », E. Jaramillo, P. Aniorté, M. Munier – 34ème Congrès INFORSID, atelier SSI (Grenoble, France, 31 mai au 3 juin 2016)
- **SARSSI 2014** – « *Métadonnées et Aspects Juridiques: Vie Privée vs Sécurité de l'Information* », M.Munier, V.Lalanne, P.Y.Ardoy, M.Ricarde – 9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (Saint-Germain-Au-Mont-d'Or (Lyon), France, 13-16 mai 2014) – pages 65-76
- **Thèse Vincent Lalanne** – « *Gestion des risques dans les architectures orientées services* » – encadrement A. Gabillon, M. Munier (soutenue le 19/12/2013)
- **PASSAT 2013** – « *Information Security Risk Management in a World of Services* », V.Lalanne, M.Munier, A.Gabillon – 2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust (Washington D.C., USA, September 8th-14th, 2013) – pages 586-593
- **DPM 2013** – « *Legal Issues about Metadata: Data Privacy vs Information Security* », M.Munier, V.Lalanne, P.Y.Ardoy, M.Ricarde – 8th International Workshop on Data Privacy Management (in conjunction with ESORICS 2013) (Egham, UK, September 12th-13th, 2013) – LNCS 8247, pages 162-177, ed. Springer (ISBN 978-3-642-54567-2)
- **WOSIS 2013** – « *Information Security in Business Intelligence based on Cloud: A Survey of Key Issues and the Premises of a Proposal* », E.Jaramillo, M.Munier, P.Aniorté – 10th International Workshop on Security in Information Systems (Angers, France, July 5, 2013)