Accords de niveau de service et modèle de réputation pour le contrôle d'usage

Elena Jaramillo Rojas[1]

LIUPPA, Université de Pau et des Pays de l'Adour
371 rue du Ruisseau – BP 201
40004 Mont de Marsan

gloriaelena.jaramillorojas@univ-pau.fr

MOTS-CLÉS : *objectifs de niveau de service, réputation, workflow inter-organisationnel, gestion de la responsabilité.*

KEYWORDS: *service-level objectives, reputation, inter-organizational workflow, accountability.*

ENCADREMENT. *Philippe Aniorté (PR) et Manuel Munier (MCF)*

1. Contexte

La sous-traitance de services est devenue une nouvelle forme d'interaction pour les entreprises en leur permettant de se concentrer sur leur cœur de métier en profitant des avantages des architectures orientées services. La collaboration résultant de cette sous-traitance entraîne la création de services composés et de workflows complexes dans lesquels le client d'un service partage des informations sensibles avec d'autres organisations externes et indépendantes. Dans un tel contexte inter-organisationnel, plusieurs défis restent à relever par la communauté. Tout d'abord, le partage explicite de données entre les différents partenaires engendre une perte de contrôle sur les données passés au(x) fournisseur(s) de service(s). Deuxièmement, la complexité de la chaîne de processus nécessite de définir des stratégies de gestion de la confiance et de gestion des responsabilités (et des pénalités) en cas de mauvaise exécution des tâches prévues. Troisièmement, la création de workflows dynamiques permet de poursuivre

1. Ce travail est soutenu par le Conseil Général des Landes (allocation de recherche)

ces interactions inter-organisationnelles malgré des comportements défectueux tout en préservant le niveau de service requis par le client. Finalement, les partenaires du workflow doivent prouver, dans leurs comportements, qu'ils respectent les politiques établies. Mais agissant comme des boîtes noires ils doivent garder leur autonomie.

Dans cet article, nous présentons une nouvelle analyse de la notion d'accord de niveau de service (SLA) appliquée au contrôle d'usage des données. Pour cela, dans la section suivante, nous détaillons les trois parties principales de notre proposition. Nous identifions ensuite les principales contributions de notre travail par rapport à l'état de l'art. La conclusion et les travaux futurs termineront cet article.

2. Problématique et actions réalisées

Les SLA sont des documents signés, consentis et convenus qui engagent à la fois le client et le fournisseur sur le respect d'une liste de conditions quant à la fourniture du service. Plusieurs approches ont été proposées pour combler l'écart entre les aspects juridiques et techniques, le problème persiste de savoir comment définir ce qu'est un niveau de service dans un environnement inter-organisationnel.

Notion de niveau de service. Savoir ce que signifie un accord de niveau de service inter-organisationnel n'est pas une question triviale, car dans ce genre d'environnements, bien que les partenaires aient convenu d'un objectif final commun, chacun d'eux possède néanmoins ses propres objectifs [1]. Suivant notre approche orientée contrôle d'usage, nous définissons le niveau de service inter-organisationnel en termes de respect des conditions d'utilisation imposées par le propriétaire des données et représentées sous la forme d'objectifs de niveau de service (SLO). Nous proposons également la notion de *niveau de service propagé* (PSL) en tant que stratégie nous permettant de lier et de surveiller les SLO entre les différents partenaires impliqués dans le workflow, et plus important encore, d'adapter et de négocier les SLO en cas de non-conformité. Nous proposons à partir de la notion de PSL que la non réalisation d'au moins un SLO par un nœud du workflow génère un effet domino sur la totalité des SLO en déclenchant un processus de négociation entre les partenaires. Nous considérons qu'avant que les données puissent être utilisées par un autre partenaire du workflow, celui-ci doit être informé de l'état du système et négocier les SLO non respectés. Cela implique que l'algorithme qui régit notre approche de PSL a en entrée les objectifs de service et produit en sortie un résultat final (si nécessaire) et la preuve de l'usage qu'il prétend avoir fait des données tout au long du workflow ; le processus est considéré comme dynamique et dépend complètement de la réalisation (ou non) des SLO. En considérant l'interaction inter-organisationnelle, trois autres composants sont impliqués, à savoir le coordinateur du workflow, le composant de négociation et le composant nommé *Universal Description Discovery and Integration* (UDDI). La principale fonction du coordinateur est de distribuer les fonctions aux nœuds, d'évaluer l'accomplissement des SLO et, en cas de comportement incorrect, d'informer le composant de négociation de la situation afin qu'il essaye, dynamiquement, de trouver dans l'UDDI un autre service qui pourrait garantir l'accomplissement des SLO au niveau global.

Niveau de service et gestion de la responsabilité. Comme il a été indiqué, la sortie du processus est un journal qui sert de preuve de l'usage qui a été fait des données à l'intérieur du workflow. Afin d'utiliser le journal comme preuve il faut qu'il ait les propriétés suivantes : (i) Il ne peut être modifié ou accessible que par des entités autorisées. (ii) Il doit détailler le flux de données complet, incluant la date à laquelle les données ont été utilisées, le but de l'utilisation, l'action effectuée avec les données ainsi que le responsable de l'action. (iii) Il doit garantir que les informations enregistrées dans le journal sont fiables en signant l'entrée du journal.

Quant à la mise en œuvre, l'architecture pourra être centralisée ou distribuée, mais il faudra que la création du journal soit être synchronisée avec l'exécution du workflow, et donc également avec le flux de données. Supposons que les données transmises soient modifiées par deux nœuds indépendants suite à un embranchement du workflow. Puisque le coordinateur du workflow connaît la configuration globale du système, il pourrait éviter les mises à jours incorrectes des données, ou les erreurs d'enregistrement ou de fusion dans le journal.

Niveau de service et réputation. Un point à prendre en compte est la façon dont le composant de négociation choisit un nouveau fournisseur de services pour l'intégrer au workflow. Nous utilisons pour cela la notion de réputation. La première fois qu'un client accède aux services d'un fournisseur, le client lui fait confiance quant à l'accomplissement des SLO convenus. Cependant, en cas de violation, le système applique une pénalité au fournisseur. Au niveau de l'architecture, la base de données contenant les informations sur la réputation de chaque entité ne pourra être accédée que par le composant de négociation afin de préserver l'intimité de l'entité, mais aussi parce que nous proposons une mesure subjective de la réputation basée sur des seuils et les sanctions établies par le client du service en tenant compte seulement de ses objectifs. Dans notre proposition nous attribuons des sanctions pour la violation de SLO liés à l'utilisation des données, mais aussi de la politique de sécurité.

3. État de l'art

Des initiatives de sécurité inter-organisationnelle comme TOrBAC [4] et Multi-Trust-OrBAC [2] incluent dans leur politique de sécurité, comme dans le présent article, un modèle de réputation. Cependant, ces travaux ne comprennent pas la notion de contrôle d'usage des données, ni n'envisagent de façon explicite le processus de négociation entre les différents partenaires impliqués dans le workflow. D'autre part, dans la littérature, plusieurs propositions abordent le problème de l'utilisation des données par un troisième partenaire. [3] propose une approche de contrôle de l'usage en fonction de conditions contextuelles qui sont vérifiées pendant et après que l'autorisation ait été accordée. D'une manière générale, à notre connaissance, le contrôle d'usage a été défini et mis en œuvre comme un accès en continu [5]. En tenant compte de l'état actuel de l'évolution de nos domaines de recherche, voici les principales contributions de notre travail : (i) Notre proposition vise à compléter les techniques d'autorisation et d'authentification traditionnelles en passant de *qui* peut

accéder à *quelles* ressources et *quand*, à *comment* les ressources sont utilisées une fois accessibles. (ii) Nous proposons une nouvelle approche de l'utilisation des SLO dans laquelle nous démontrons le phénomène de niveau de service propagé. (iii) Nous mettons en œuvre notre notion de niveau de service propagé pour créer des workflows dynamiques et pour déterminer un degré de réputation pour chaque partenaire.

4. Conclusion

Comment faire pour contrôler les données qui sont partagées ou fournies à un prestataire externe est un domaine de recherche actif dans le monde entier en raison des implications juridiques et commerciales. Dans cet article nous présentons notre proposition de contrôle d'usage des données sur la base de relations contractuelles entre les entités manipulant ces données. Nous visons à établir une chaîne de responsabilités dans l'exécution d'un workflow en créant des journaux, mais aussi avec l'application d'une stratégie de sanctions sur la base de la violation de la politique de sécurité et des objectifs de niveau de service convenus quant à l'utilisation des données. Nous proposons aussi l'applicabilité des niveaux de service propagés dans un workflow inter-organisationnel.

5. Actions futures

La prochaine étape consiste à intégrer et à formaliser les SLO en tant qu'éléments de la politique de sécurité inter-organisationnelle. Notre idée initiale est orientée vers l'utilisation d'OrBAC ou d'une de ses variantes telles que Multi-Trust-OrBAC [2] et inclue de nouveaux éléments liés au but de l'utilisation des données, en proposant également une nouvelle catégorie pour les conditions contextuelles associées à l'utilisation des données dans un environnement inter-organisationnel.

Bibliographie

[1] Munier M., Lalanne V., Ardoy P-Y., Ricarde, M., Legal Issues about Metadata Data Privacy vs Information Security, DPM 2013.

[2] Ben Saidi, M., Marzouuk A., Multi-Trust-OrBAC : Access Control Model for Multi-Organizational Critical Systems Migrated to the Cloud, 2013.

[3] Sans, T., Cuppens, F., and Cuppens-Boulahia, N., A Framework to Enforce Access Control, Usage Control and Obligations, Annales Des Télécommunications. 2007.

[4] El Kalam A.A., Marzouk A., TOrBAC : A Trust Organization Based Access Control Model for Cloud Computing Systems, 2012.

[5] Pretschner, A. and Schütz, F. and Schaefer, C. and Walter, T.. Policy Evolution in Distributed Usage Control. Electron. Notes Theor. Comput. Sci.2009