Contrôle d'accès dans une plate-forme PaaS (Audit)

Ahmed BOUCHAMI, Olivier PERRIN, LORIA

Introduction

La sécurité d'une plate-forme collaborative nécessite un module d'authentification et un module de contrôle d'accès. Le premier sert à savoir qui est l'utilisateur courant (son identité au sein de la plateforme), et le second à connaître son rôle et s'il est autorisé à faire une certaine action (a-t-il accès aux ressources qui peuvent être partagée).

Les collaborations au sein des plateformes collaboratives sont souvent réalisées dans plusieurs sessions en fonction de l'instant de réalisation des tâches collaboratives, l'état d'avancement, mais également au nombre et/ou la nature des participants. Par conséquent, il s'avère intéressant d'évaluer la qualité de la collaboration après la fin de chaque session collaborative. Cela peut bien contribuer d'une manière directe à l'amélioration de la qualité du travail collaboratif réalisé, ainsi qu'à la sécurité de la plateforme d'une manière indirecte.

Actuellement, es systèmes de recommandations suscitent beaucoup d'intérêt. Ces systèmes se basent principalement sur l'analyse des critiques des utilisateurs vis-à-vis d'une entité (produit, service ou fournisseur, vendeur...) suite à leurs expériences à l'égard de cette dernière.

L'idée dans OpenPaas est de réutiliser ce principe de recommandation et de notation pour l'audit et la gouvernance de la sécurité de la PaaS de telle sorte qu'elle renforce nos objectifs en terme de sécurité.

1 Réputation et Confiance numérique

La confiance numérique (*trust*) et la réputation électronique sont deux concepts relatifs dont on trouve dans la littérature plusieurs définitions. La définition de la

e-reputation donnée par *wikipédia* est la suivante : *l'e-réputation, aussi appelée web-réputation, cyber-réputation, réputation numérique, sur le Web, sur Internet ou en ligne, est la réputation, l'opinion commune (informations, avis, échanges, commentaires, rumeurs...) sur le Web d'une entité (marque, personne, morale (entreprise) ou physique (particulier), réelle (représentée par un nom ou un pseudonyme) ou imaginaire. Elle correspond à l'identité de cette entité associée à la perception que les autres s'en font.* Une autre définition donnée par *Riedl* est la suivante: ≪*le trust est nécessaire en raison de l'impossibilité de traiter le monde dans sa pleine complexité, l'impossibilité d'éviter cette complexité complètement et l'impossibilité de se protéger complètement contre tous risques de mauvais comportements d'autrui*≫ [2].

L'e-réputation est un concept qui se développe progressivement avec l'utilisation de plus en plus large des réseaux sociaux. Elle sert à évaluer d'une manière proactive le comportement des individus, entreprises ainsi que des services. Cela est important, car cela permet aux utilisateurs d'avoir une idée sur le taux de confiance qu'ils peuvent accorder à leurs futurs collaborateurs. La principale problématique à laquelle sont confrontés les systèmes de recommandation par rapport à la e-réputation concerne la non crédibilité des informations (critiques et notes) collectées. En effet, le système ne peut pas savoir si une entité évalue **correctement** les autres entités avec lesquelles elle interagit.

Une solution peut être la conception de systèmes d'évaluation **automatiques** qui se base sur des règles d'évaluations bien précises. Cette solution peut être facilement intégrée dans l'architecture de sécurité de OpenPaaS afin d'auditer la sécurité et de faciliter la gouvernance.

2 Le trust dans OpenPaaS

La définition la plus simple du trust et ses concepts reliés est la suivante [3]:

- **trust**: croyance qu'on offre à un quelqu'un afin qu'il puisse réaliser des actions, de telle sorte qu'il nous déçoit pas,
- **trustworthiness (taux de confiance)**: mesure de trust (valeur) qui reflète le niveau de relation de confiance entre deux (ou plusieurs) collaborateurs,
- **reputation**: mesure déduite à partir des comportements des utilisateurs. Elle est utilisée pour évaluer le *trustworthiness* qu'un utilisateur accorde à un autre.

Comme nous l'avons déjà mentionné, l'évaluation de la confiance numérique peut renforcer les mécanismes de sécurité dédiés à une plateforme collaborative. L'architecture de contrôle d'accès prévue pour OpenPaaS se basera principalement sur des **STS** (cf. livrable autorisation). Par conséquent, l'intégration de système d'évaluation automatique au sein des **STS** peut être très avantageuse. Cela permettra de pallier le problème concernant les évaluations mutuelles **bruitées** des collaborateurs.

L'idée consiste à définir un mécanisme capable, après la fin de chaque session collaborative, d'évaluer la qualité de la collaboration vis-à-vis de chaque membre de la session collaborative. Cela pourra être possible en se basant sur des conventions pré-établies par les membres faisant partie de la session. Ces conventions pourraient dépendre du comportement des collaborateurs, des résultats attendus, des délais respectés.... En possédant ces informations, on pourrait envisager par exemple que les évaluations puissent engendrer:

- des modifications au niveau des droits d'accès, via l'ajout et/ou la suppression d'une ou plusieurs facettes à l'égard d'un ou plusieurs collaborateurs,
- l'utilisation de la recommandation d'un utilisateur afin qu'il puisse intégrer (ou non) une session (les membres se basant sur la e-réputation de ce dernier pour décider de l'intégrer ou le rejeter),
- l'exclusion d'un collaborateur appartenant à une session en cours suite à une mauvaise collaboration ou tentative de fraude.

Techniquement, l'évaluation se fait grâce à une analyse d'un ensemble de données contenant des informations relatives aux sessions collaboratives. Ces données peuvent par exemple être extraites des fichiers de **log**.

2.1 Audit des fichiers de logs

Les logs sont des fichiers contenant l'historique des événements survenus lors d'une ou plusieurs session collaboratives au sein de la PaaS. Ils contiennent des messages, des avertissements, des erreurs enregistrées, des tentatives de connexion échouées, des tentatives d'accès à des ressources protégées... Ils permettent à un système d'audit de tracer les comportements des utilisateurs et du système afin de pouvoir évaluer leurs attitudes ainsi que leurs actions. D'un point de vue sécurité, ils peuvent servir d'indicateurs pour la détection de fraudes. Ils peuvent également servir à calculer les valeurs du trust dans la plateforme collaborative.

Afin de pouvoir analyser les logs, les techniques de **data-mining** [1] peuvent être très intéressantes dans la perspective d'un passage à l'échelle. Cependant,

afin de bien exploiter les logs, il est préférable que ces derniers soient bien structurés. Par conséquent, il faudra essayer de définir grâce à un format standard (e.g. XML) une structure spécifique aux logs de la plateforme définissant les attributs nécessaires au(x) module(s) d'audit dédié(s) à OpenPaaS.

Par conséquent, il est nécessaire de proposer une méthode de collecte de logs depuis les **STS**. L'analyse des logs peut être appliquée de plusieurs manière. Cela dépendra de la manière dont les **STS** vont être appliqués (cf. proposition d'architecture).

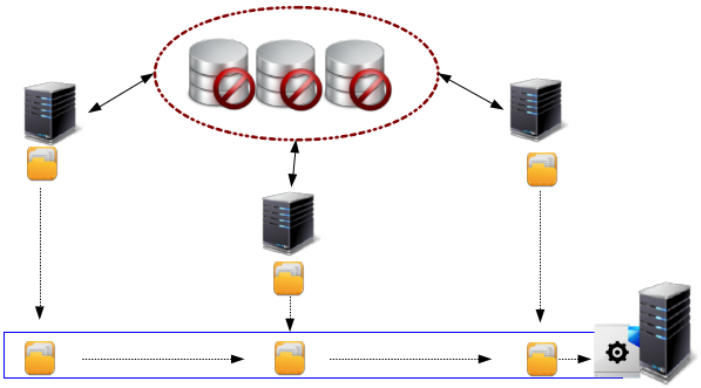

Figure 1: *Vue globale modèle centralisé d'analyse de logs*

Les logs vont servir à prendre des décisions, ce qui implique qu'ils doivent être exploités par le module de prise de décision au niveau des *STS* d'une manière optimale, que celle-ci soit centralisée ou bien distribuée, avec une bonne synchronisation entre les *STS*.

Conclusion

Dans ce manuscrit, nous avons discuté la possibilité de renforcer le modèle de sécurité destiné à OpenPaaS en intégrant de nouvelles informations. Nous avons proposer d'intégrer le concept de *trust* qui consiste à évaluer la qualité de la collaboration ainsi qu'à surveiller les événements qui ont lieu au sein de la plateforme. Ce concept se base principalement sur l'analyse des logs contenants des informations sur les sessions collaboratives, et met en jeu à la fois des techniques basées sur le *Complex Event Processing* (CEP) et sur le mining de ces événements.

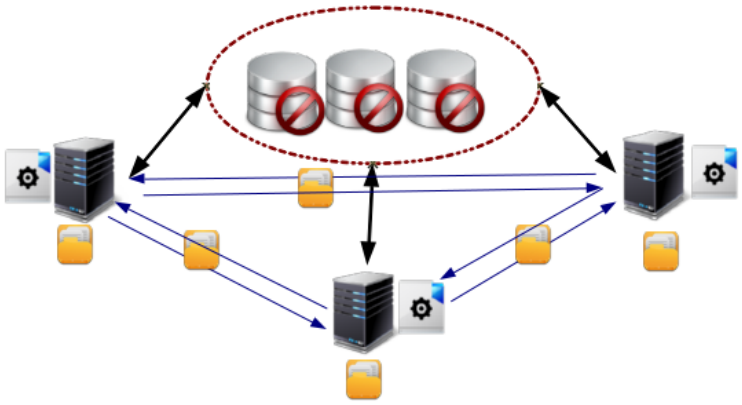

Figure 2: *Vue globale modèle décentralisé d'analyse de logs*

Pour pouvoir traiter cette nouvelle problématique, nous pensons utiliser les techniques de **data mining** afin d'être en mesure de fouiller des grandes quantités d'informations issues des logs de la PaaS pour en extraire les informations liées à la sécurité à travers les actions collaboratives engendrées par les participants.

References

[1] Rakesh Agrawal, Dimitrios Gunopulos, and Frank Leymann. *Mining process models from workflow logs*. Springer, 1998.

[2] Reinhard Riedl. Rethinking trust and confidence in european e-government. *White paper*, 2004.

[3] Hien Thi Thu Truong. *Un mod èle de collaboration bas é sur les contrats et la con fiance*. PhD thesis, Université de Lorraine, 2012.