HAL
open science

Mécanisme de réputation distribué préservant la vie privée avec témoignages négatifs

Paul Lajoie-Mazenc, Emmanuelle Anceaume, Gilles Guette, Thomas Sirvent, Valérie Viet Triem Tong

To cite this version:

Paul Lajoie-Mazenc, Emmanuelle Anceaume, Gilles Guette, Thomas Sirvent, Valérie Viet Triem Tong. Mécanisme de réputation distribué préservant la vie privée avec témoignages négatifs. ALGOTEL 2015 - 17èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, Jun 2015, Beaune, France. hal-01148072

HAL Id: hal-01148072

https://hal.science/hal-01148072v1

Submitted on 4 May 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Mécanisme de réputation distribué préservant la vie privée avec témoignages négatifs

Paul Lajoie-Mazenc[1] and Emmanuelle Anceaume[2] and Gilles Guette[1] and Thomas Sirvent[3] and Valérie Viet Triem Tong[4]

[1] *IRISA / Université de Rennes 1*
[2] *IRISA / CNRS*
[3] *IRISA / DGA Maîtrise de l'Information*
[4] *IRISA / CentraleSupélec*

Les mécanismes de réputation permettent de réduire les risques pris par les utilisateurs dans les réseaux ouverts et à large-échelle en associant un *score de réputation* aux utilisateurs, qui résume leur comportement passé. Néanmoins, pour atteindre leur objectif, ces mécanismes peuvent mettre en danger la vie privée de leurs utilisateurs. Des solutions préservant la vie privée de leurs utilisateurs ont été proposées ; cependant, elles n'offrent pas de garanties de vie privée assez fortes, ou réduisent l'utilité de la réputation. Dans cet article, nous proposons un mécanisme de réputation distribué préservant la vie privée, tout en permettant aux clients de témoigner positivement ou négativement ; cette proposition repose à la fois sur des outils cryptographiques et des tierces parties distribuées. Nous montrons également que notre proposition est efficace, et donc utilisable en pratique.

Keywords: Systèmes distribués, Mécanismes de réputation, Vie privée, Cryptographie appliquée

1 Introduction

Les mécanismes de réputation sont devenus des outils puissants permettant d'instaurer la confiance dans des réseaux où les utilisateurs ne se connaissent pas, par exemple dans le cadre du commerce électronique. Les clients témoignent sur les fournisseurs de service avec lesquels ils interagissent, ce qui permet aux autres utilisateurs de savoir comment se comportent ces fournisseurs sans les connaître. Ces mécanismes sont généralement distribués, ce qui évite qu'une autorité centrale ne contrôle les réputations de tous les fournisseurs de service, et ne soit un point unique de défaillance du système.

Cependant, les mécanismes de réputation requièrent de nombreuses informations personnelles pour atteindre ce but : le témoignage d'un client sur un fournisseur permet de connaître la fréquence des interactions du client, leur type, etc. C'est pour cette raison que des mécanismes de réputation préservant la vie privée sont apparus. Les premiers mécanismes visaient à préserver le secret des témoignages des clients, pour éviter qu'un fournisseur ne puisse exercer de représailles sur un client l'ayant mal noté. Hasan et coll. [HBBS13] proposent une telle approche, tolérant les comportements byzantins des fournisseurs ainsi que des clients tout en préservant le secret des témoignages : une fois qu'un client a témoigné, il est impossible de savoir si ce témoignage est positif ou négatif. Cependant, la vie privée des clients eux-mêmes n'est pas préservée, et un fournisseur est toujours capable de discriminer un client sur la base de son identifiant.

Des mécanismes garantissant des propriétés de vie privée plus fortes sont donc apparus. Par exemple, Bethencourt et coll. [BSS10] proposent un mécanisme garantissant un anonymat total des clients et des fournisseurs. En outre, ce mécanisme permet de repérer les *bourrages d'urne* ; en effet, un client ne doit pas être capable de témoigner de nombreuses fois sur un fournisseur pour augmenter artificiellement sa réputation. Ainsi, les auteurs proposent d'*associer* les témoignages sur un même fournisseur, afin de ne prendre en compte qu'un seul témoignage par client. C'est-à-dire qu'ils proposent un moyen permettant de vérifier si deux témoignages ont été émis par un même client – sans dévoiler ce client. Cependant, ce mécanisme a deux inconvénients majeurs. Premièrement, les clients ne peuvent témoigner des mauvais comportements ;

la réputation des fournisseurs ne peut pas diminuer. Deuxièmement, un fournisseur a besoin de 500 ko par témoignage reçu pour prouver sa réputation à un client potentiel : ce mécanisme est inefficace.

Dans cet article, nous proposons un mécanisme de réputation efficace préservant la vie privée des clients et des fournisseurs, permettant aux clients d'émettre des témoignages positifs et négatifs. La Section 2 motive les propriétés nécessaires à un tel mécanisme, tandis que la Section 3 fournit une description haut-niveau de notre proposition.

2 Propriétés de vie privée et de sécurité

Préserver la vie privée des utilisateurs réduit les discriminations : les clients ne doivent pas être capables de cibler un fournisseur particulier pour médire sur lui, et réciproquement. Il faut donc éviter qu'un client ne connaisse l'identité d'un fournisseur au moment où il témoignage ; de cette manière, l'identité du fournisseur n'a aucune influence sur le témoignage. Similairement, les fournisseurs ne doivent pas savoir qui sont leurs clients pendant les transactions. En outre, si deux fournisseurs ou plus combinent les informations à propos de leurs témoins, ils peuvent potentiellement tracer ces clients. Il faut donc assurer que les clients de différents fournisseurs ne peuvent être associés.

Notre mécanisme doit également garantir des propriétés de sécurité. Tout d'abord, rappelons que les clients doivent être en mesure d'émettre des témoignages négatifs. Il faut donc assurer que, si un client désire émettre un témoignage négatif, le fournisseur avec qui il interagit ne peut l'en empêcher : c'est l'*indéniabilité des témoignages*. Similairement, les clients peuvent omettre de témoigner, volontairement ou non. Afin de calculer un score de réputation représentatif du comportement des fournisseurs de service, il faut que les fournisseurs puissent obtenir un témoignage par défaut quand le client refuse d'en émettre un. Il faut également garantir qu'un utilisateur malveillant, à l'intérieur d'une collusion ou pas, est incapable de forger un témoignage qui n'aie pas été émis à l'issue d'une transaction légitime, ou un score de réputation qui ne soit pas son score de réputation légitime. Finalement, nous avons expliqué précédemment qu'un client pouvait émettre de nombreux témoignages sur un unique fournisseur afin d'augmenter considérablement sa réputation. Lorsque les clients sont complètement anonymes, de tels bourrages d'urne ne peuvent être évités. C'est pourquoi, à l'instar du mécanisme de Bethencourt et coll. [BSS10], il faut permettre d'associer les témoignages sur un même fournisseur.

Pour résumer, un mécanisme de réputation préservant la vie privée de ses utilisateurs doit garantir les cinq propriétés suivantes : (1) la vie privée des fournisseurs est préservée ; (2) celle des clients également ; (3) un client ou un fournisseur ne peut pas dénier un témoignage ; (4) les témoignages et scores de réputation sont inforgeables ; (5) les témoignages multiples sont détectés.

3 Description de notre mécanisme

Nous présentons maintenant notre mécanisme de réputation. Dans un premier temps, nous expliquons pourquoi utiliser deux tierces parties de confiance, et comment les choisir. Nous décrivons ensuite une interaction. Finalement, nous montrons que ce mécanisme est efficace.

3.1 Tierces parties distribuées

Gestion des témoignages Les clients doivent pouvoir émettre des témoignages négatifs. Les fournisseurs ne peuvent pas gérer eux-mêmes les témoignages qu'ils reçoivent ; en effet, les fournisseur peuvent alors simplement « oublier » les témoignages négatifs reçus afin d'améliorer leur réputation. Ainsi, il faut qu'une tierce partie stocke les témoignages. De plus, les fournisseurs doivent être anonymes ; un client ne doit pas être capable de distinguer deux fournisseurs parce que leurs témoignages sont gérés par deux tierces parties différentes. Ainsi, la gestion des témoignage impose une tierce partie de confiance qui soit *unique* pour tous les fournisseurs. Cette tierce partie est responsable des scores de réputation des fournisseurs, et atteste leur calcul. Notons qu'elle n'a pas besoin d'être en ligne en permanence : il est suffisant qu'elle signe les réputations à intervalles de temps réguliers.

Garantie de l'indéniabilité L'indéniabilité des témoignages et la vie privée des utilisateurs peuvent paraître contradictoires ; en effet, le client ne doit pas connaître le fournisseur au moment où il choisit son

témoignage, mais il doit pouvoir émettre son témoignage sur le fournisseur – et donc connaître l'identifiant du fournisseur – une fois choisi. Nous proposons d'utiliser une tierce partie de confiance garantissant l'émission des témoignages. Il ne faut pas que chaque utilisateur composant cette tierce partie connaisse l'identifiant du fournisseur : dans ce cas, si le client est en collusion avec un seul de ces utilisateurs, il peut connaître l'identifiant du fournisseur. À cet effet, nous utilisons un schéma de partage de secret. Ainsi, chaque composant de la tierce partie reçoit une seule part du secret, qui ne donne aucune information. En cas de besoin, les parts peuvent être combinées pour reconstruire le secret. Notons que, bien que cette tierce partie doive être en ligne pour assister les transactions, elle n'a pas besoin d'être unique pour toutes les transactions.

Nous pourrions choisir d'utiliser une seule tierce partie pour remplir les deux rôles. Cependant, ceux-ci nécessiteraient d'avoir une tierce partie unique pour tous les fournisseurs et transactions, et en ligne. Une telle tierce partie requerrait trop de ressources dans un système large-échelle. Nous proposons donc une première tierce partie, les *signataires accrédités*, gérant les scores de réputation, et une deuxième, les *porteurs de part*, garantissant l'émission des témoignages.

Choix des tierces parties Les signataires accrédités sont responsables du calcul de tous les scores de réputation, et sont donc cruciaux au fonctionnement du mécanisme de réputation. Pour cette raison, nous proposons de choisir les fournisseurs de service gérant les plus gros volumes de transactions. Le choix des porteurs de part est différent. En effet, ils sont choisis aléatoirement pour chaque transaction parmi les fournisseurs de service. Le client et le fournisseur se mettent d'accord sur un nonce aléatoire, et les porteurs de part sont ensuite choisis en itérant une fonction de hachage H sur ce nonce. S'il y a N porteurs de part possible, les n porteurs de part choisis en utilisant le nonce nonce sont les $\{H(\mathsf{nonce}\|i) \times N/2^h, 1 \leqslant i \leqslant n'\}$ où H est une fonction de hachage dont les sorties font h bits, et n' est choisi afin qu'il y ait n porteurs de part différents dans l'ensemble résultant. Le nombre de porteurs de part nécessaires peut être modélisé par une distribution hypergéométrique, dépendant de plusieurs paramètres : le nombre d'utilisateurs, la proportion d'utilisateurs malveillants, ainsi que la probabilité maximale désirée d'obtenir une collusion. La figure 1 présente le nombre de porteurs de part nécessaires pour une telle probabilité de 2^{-20}, c'est-à-dire environ 10^{-6}. Cette figure montre d'une part que le système passe à l'échelle, et d'autre part que le nombre de porteurs de part nécessaire reste acceptable.

3.2 Ébauche du protocole d'interaction

Une interaction entre un client et un fournisseur se déroule en trois étapes.

Preuve de réputation À intervalles de temps réguliers, chaque fournisseur de service reçoit une signature des signataires accrédités portant sur sa réputation. Cette signature est une signature proxy anonyme [FP08], ce qui permet au fournisseur d'en masquer certains éléments. Le fournisseur peut notamment masquer son identité pour éviter de révéler son identité, et préserver sa vie privée.

Partage de secret Une fois qu'un client a vérifié la réputation du fournisseur qui l'intéresse, ils choisissent ensemble un nonce leur permettant de choisir les porteurs de part. Pour ce faire, ils utilisent un protocole de tirage au sort sécurisé pour empêcher le client et le fournisseur de contrôler le nonce, et donc les porteurs de part. Une fois que les porteurs de part ont été choisis, le client et le fournisseur utilisent le schéma de partage de secret pour garantir l'indéniabilité des témoignages à leur partenaire. Le schéma de partage de secret utilisé est plus précisément *vérifiable*, afin de garantir que le bon secret sera reconstruit. Une fois que les partages ont été vérifiés, le fournisseur et le client peut procéder à la transaction.

Émission du témoignage Après la transaction, le client et le fournisseur émettent le témoignage. Il y a alors trois scénarios, suivant leur comportement : (A) le fournisseur et le client participent ; (B) le client ne participe pas ; (C) le fournisseur ne participe pas. Dans le premier cas, le client commence par choisir ton témoignage. Le fournisseur révèle ensuite son identifiant, ce qui permet l'émission du témoignage. Dans le deuxième cas, le fournisseur peut construire le témoignage grâce aux porteurs de part. Dans le dernier cas, le client choisit son témoignage avant d'obtenir l'identifiant du fournisseur via les porteurs de part.

Calcul des réputations À intervalles de temps réguliers, les signataires accrédités récupèrent tous les témoignages, et mettent à jour les scores de réputation des fournisseurs. Finalement, ils signent les réputations des fournisseurs en utilisant des signatures proxy anonymes.

3.3 Performances du mécanisme

Pour évaluer les performances du système, toutes les opérations cryptographiques effectuées par chaque utilisateur au cours d'une interaction sont comptées. En utilisant des temps de référence, il est ensuite possible d'évaluer le temps de calcul nécessaire à chaque utilisateur. La figure 2 présente ces temps, pour un système comprenant un signataire accrédité et 28 porteurs de part, ce qui suffit à empêcher les collusions avec une probabilité 2^{-20} dans un système de 10^8 utilisateurs, dont 5% de malveillants. Comme le montre cette figure, les temps de calcul sont réalistes et permettent une implémentation pratique de ce mécanisme. Le nombre de signataires accrédités pourrait même être augmenté : le seul temps dépendant de ce nombre correspond à la preuve de réputation, et en dépend linéairement. Pour 25 signataires accrédités, la preuve de réputation demande 401 ms au client et 268 ms au fournisseur. De plus, dans le pire cas, les utilisateurs n'échangent que 300 ko pendant une interaction complète, ce qui prouve l'efficacité du mécanisme.

4 Conclusion

Dans cet article, nous avons décrit un mécanisme de réputation distribué préservant la vie privée de ses utilisateurs, qui permet également aux clients d'émettre des témoignages négatifs, tout en étant efficace. Cette approche, décrite précédemment [AGL+14], montre qu'un compromis acceptable entre réputation et vie privée peut être atteint.

Dans le futur, nous prévoyons d'étudier une variante optimiste de notre mécanisme, qui ne nécessite les porteurs de part que lorsque le client ou le fournisseur refuse de participer à l'émission du témoignage.

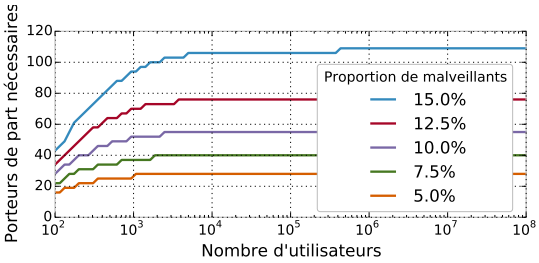

FIGURE 1: Nombre de porteurs de part nécessaires

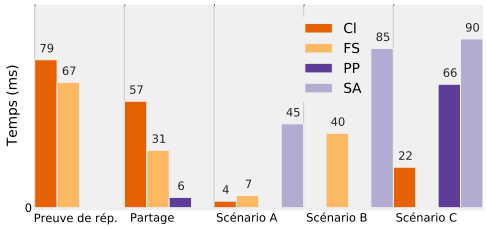

FIGURE 2: Temps de calcul des utilisateurs pendant chaque étape d'une interaction

Références

[AGL+14] Emmanuelle Anceaume, Gilles Guette, Paul Lajoie-Mazenc, Thomas Sirvent, and Valérie Viet Triem Tong. Extending signatures of reputation. In *Privacy and Identity Management for Emerging Services and Technologies*, pages 165–176. Springer Berlin Heidelberg, 2014.

[BSS10] John Bethencourt, Elaine Shi, and Dawn Song. Signatures of reputation. In *Financial Cryptography and Data Security (FC)*, pages 400–407. Springer Berlin Heidelberg, 2010.

[FP08] Georg Fuchsbauer and David Pointcheval. Anonymous proxy signatures. In *Security and Cryptography for Networks (SCN)*, pages 201–217. Springer Berlin Heidelberg, 2008.

[HBBS13] Omar Hasan, Lionel Brunie, Elisa Bertino, and Ning Shang. A decentralized privacy preserving reputation protocol for the malicious adversarial model. *IEEE Transactions on Information Forensics and Security*, 8(6) :949–962, 2013.