Étude du contrôle sur les données personnelles dans GNU Taler à l'aide de Capacity

Pablo Rauzy <pr@up8.edu>
Université Paris 8 / LIASD & GÉODE

Contexte

L'objectif de ce stage est d'utiliser le cadre formel Capacity [LMR18] pour modéliser, étudier, et caractériser le contrôle sur les données personnelles offert par le système de transaction GNU Taler [BDGS16].

GNU Taler. GNU Taler [1] est un système de paiement respectueux de la vie privée : les acheteur·ices peuvent rester anonymes, et pourtant les commerçant·es ne peuvent pas dissimuler leurs revenus perçus avec GNU Taler. Cela contribue à lutter contre la fraude fiscale et le blanchiment d'argent, tout en garantissant le respect de la vie privée des personnes. Le cas d'usage de GNU Taler est le paiement, qui s'effectue toujours avec une monnaie existante (GNU Taler n'est pas d'un moyen de stocker de la valeur).

Plus concrètement, GNU Taler est une collection de logiciels (bureau de change, application marchande, portefeuille client) qui manipule des données personnelles de paiement. Ces logiciels sont libres et documentés, aussi bien pour les développeur·es, sysadmin, et utilisateur·ices [2] que pour les chercheur·es [3].

Capacity. Le droit à la vie privée ne peut plus se résumer au "droit d'être laissé tranquille". Aujourd'hui il s'agit avant tout de laisser aux utilisateur·ices de systèmes d'informations le contrôle sur leurs données personnelles. Un cadre formel permettant la modélisation, la caractérisation, et l'évaluation de ce contrôle a été proposé [LMR18]. Trois axes de contrôle ont été identifiés dans la littérature juridique [LLM15] :

— la capacité à effectuer des actions sur ses données personnelles,
— la capacité à empêcher des tiers d'effecteur des actions sur ses données personnelles, et
— la capacité à être informé des actions effectuées par des tiers sur ses données personnelles.

Dans Capacity, il y a des *agents* qui peuvent effectuer des *actions* (qui sont des *opérations* sur des *ressources* dans un *contexte* donné). Le contrôle est alors modélisé comme une *exigence*, qui exprime par une relation logique simple des contraintes sur des actions réalisables par des agents. Cette unique relation permet de modéliser les trois axes de contrôles cités ci-dessus.

La simplicité et la généricité de Capacity ne sont pas un frein à l'étude de systèmes tout à fait concrets. Capacity donne une sémantique aux exigences au travers de propriétés abstraites de traces. Ces propriétés abstraites peuvent être concrétisées pour un système donné après avoir identifié les agents, les ressources, les opérations, les contextes, et les évènements concrets qui composent les traces dans le système en question.

Dans le cadre du projet ReComp [4], une implémentation de Capacity est en cours de développement en programmation logique (*Answer Set Programming*). Elle doit permettre de vérifier la conformité d'une trace à une exigence, ainsi que de calculer, à partir d'une trace, la politique de contrôle effectivement mise en œuvre.

Objectifs du stage

Mise en œuvre de GNU Taler. La première étape de ce stage sera de réaliser une installation complète du système GNU Taler (voir Fig. 1) : un bureau de change, un marchand, et un portefeuille. La mise en œuvre et l'utilisation de GNU Taler permettront dans un premier temps de se familiariser avec le système et son fonctionnement.

1. https://taler.net/fr/
2. https://taler.net/fr/docs.html
3. https://taler.net/fr/bibliography.html
4. https://research.nii.ac.jp/RECOMP/

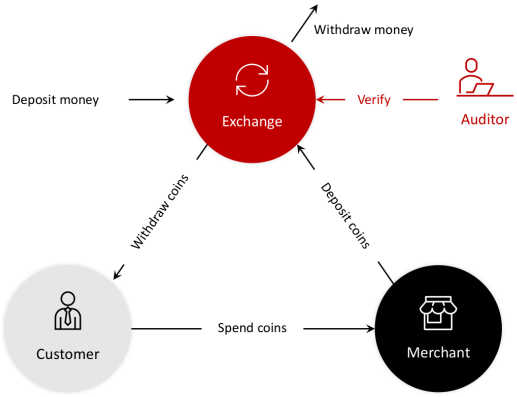

FIGURE 1 – Schéma de fonctionnement de GNU Taler.

Modélisation dans Capacity. La seconde étape consistera en la modélisation de GNU Taler dans Capacity. Cela nécessitera notamment d'identifier clairement les agents, les ressources, et les opérations, ainsi que de définir à quels évènements concrets correspondent les actions définies dans le modèle Capacity. Idéalement, il faudrait dès cet étape modéliser également l'exigence de contrôle, c'est-à-dire de privacy, que GNU Taler annonce offrir à ses utilisateur·ices.

Instrumentalisation de GNU Taler. La troisième étape consiste à instrumentaliser les implémentations des différents modules de notre installation de GNU Taler pour les faire générer des traces d'évènements concrets permettant de suivre tout ce qui se passe dans le système, notamment avec les données personnelles de ses utilisateur·ices.

Caractérisation du contrôle avec Capacity. Enfin, la dernière étape consistera à utiliser les traces d'évènement concrets générées à l'étape précédentes avec l'implémentation de Capacity pour calculer l'exigence de contrôle sur les données personnelles de ses utilisateur·ices effectivement mise en œuvre par GNU Taler, et ainsi caractériser le niveau de privacy concrètement offert par le système et étudier sa conformité à la politique de respect de la vie privée formulée par le projet GNU Taler.

Informations pratiques

Candidatures. Le ou la candidat·e idéal·e est étudiant·e en M1 ou M2 informatique (ou équivalent), a des appétences pour la formalisation et l'abstraction, ainsi que des compétences en programmation et en administration système. Seront également appréciés des connaissances et intérêts personnels pour les libertés numériques et la privacy.
Candidatures à envoyer à Pablo Rauzy <pr@up8.edu> avec un CV et une lettre de motivation.

Accueil. Le stage se déroulera dans l'équipe PASTIS [5] du LIASD à l'Université Paris 8 (Saint-Denis, 93). Le stage peut commencer entre janvier et avril 2023 et durera 5 ou 6 mois. Un bureau sera mis à disposition du ou de la stagiaire et un ordinateur portable sera fourni pour la durée du stage, si besoin. La rémunération correspond à la gratification de stage en vigueur (3,90€/heure soit ∼600€/mois).

Références

[BDGS16] J. Burdges, F. Dold, C. Grothoff, and M. Stanisci. Enabling Secure Web Payments with GNU Taler. In *6th International Conference on Security, Privacy and Applied Cryptographic Engineering, SPACE*, 2016.

[LLM15] Christophe Lazaro and Daniel Le Métayer. Control over Personal Data : True Remedy or Fairy Tale ? *SCRIPTed*, 2015.

[LMR18] Daniel Le Métayer and Pablo Rauzy. Capacity : an Abstract Model of Control over Personal Data. In *Conference on Data and Application Security and Privacy, CODASPY*, 2018.

5. https://informatique.up8.edu/pastis/