PProx

Simon Da Silva

Les plateformes de streaming vidéo (telles que YouTube, Vimeo ou Dailymotion), proposent des recommandations de contenus aux utilisateurs afin de les conserver sur leur site ou application. Pour cela, elles peuvent soit établir des profils d'intérêts pour les utilisateurs, soit dépendre de services de recommandations externes. Le calcul de ces recommandations est toujours basé sur l'historique de navigation, et parfois sur des données entrées par les utilisateurs. Cela pose donc des menaces à la *vie privée*, puisque (i) les fournisseurs de service collectent des données personnelles, (ii) un attaquant peut intercepter les recommandations et déduire des informations privées sur l'utilisateur, et (iii) des plateformes malveillantes peuvent cibler des utilisateurs spécifiques avec de la publicité pour générer des revenus, au lieu de les segmenter par groupes d'intérêts.

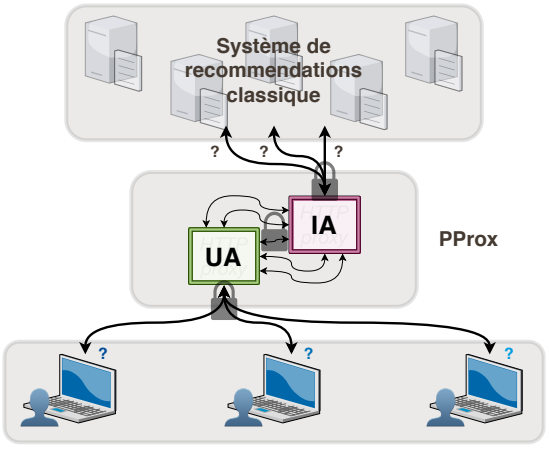
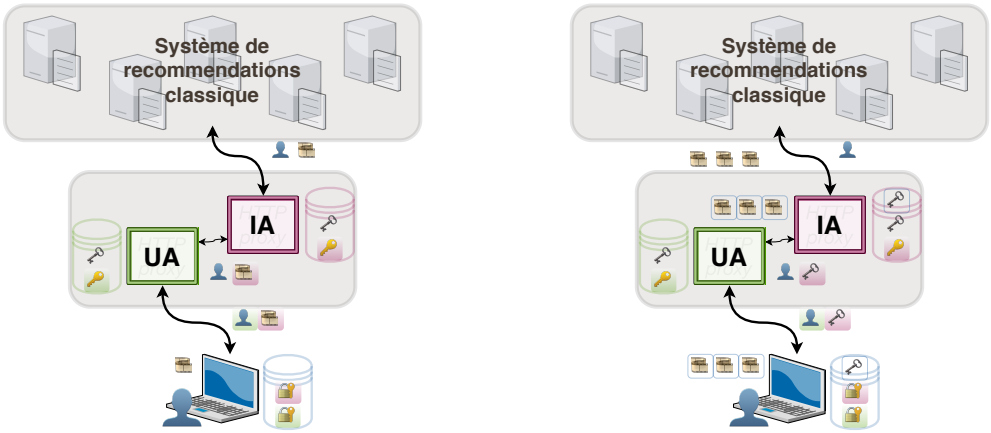


FIGURE 1 – Vue d'ensemble de PProx

PProx est une solution pragmatique permettant de fournir un service de recommandations aux utilisateurs des plateformes de streaming tout en préservant leur *vie privée*, en garantissant un anonymat total. PProx permet une bonne *qualité*

d'expérience puisqu'il n'impacte pas la précision ou la nature des recommandations, et peut être déployé avec des contraintes minimales. Il dépend d'un système de double proxy dans des enclaves Intel SGX, situé entre l'utilisateur et le service de recommandations, qui chiffre et anonymise les requêtes à la volée de manière transparente. Il mélange également les requêtes des différents clients afin de casser définitivement le lien entre les utilisateurs et les contenus qu'ils visionnent ou reçoivent comme recommandation (voir Figure 1). Ce principe est robuste aux attaques de type *side-channel*, et même à la compromission d'une des enclaves. `PProx` passe à l'échelle de manière élastique et dynamique sur un réseau de machines disposant d'enclaves Intel SGX.



(a) `PProx` - Insertion d'un élément (b) `PProx` - Envoi des recommandations

Nous avons connecté `PProx` avec le système de recommandations intégré dans Harness et l'avons évalué sur un cluster de 27 machines. Les résultats démontrent la capacité de `PProx` à gérer un grand nombre de requêtes avec une faible latence (moins de 100ms contre plusieurs secondes pour les systèmes similaires actuels), permettant d'atteindre la charge maximale supportée par le système de recommandations avec un surcoût acceptable (seulement 30% à 50% de nœuds en plus).