Algorithme de cryptpression de logs

Amazones a développé dans le cadre du projet ANR Lise, un outil d'enregistrement des traces d'exécution d'applications Java orientées service. Le principe est d'enregistrer les caractéristiques de chaque appels de service. L'infrastructure tourne actuellement sur le framework OSGi.

Les logs ainsi enregistrés représentent l'intégralité faite de l'utilisation du système par un utilisateur. Le principe est de pouvoir fournir ces traces en cas de litige de fonctionnement du système (cf article icse en biblio). Comme l'intégralité de l'activité de l'utilisateur est potentiellement faite sur l'équipement , il est nécessaire de mettre en place un algorithme de crypto robuste et adapté.

Le frein que nous voulons lever est lié à la compression des logs. Le système enregistre les activités de l'utilisateur sur un environnement mobile style smartphone, et on ne peut pas se permettre de lui remplir son disque dur de traces d'activités. La compression est donc la solution directe, mais compresser un flux de log crypté est impossible, car antagonistes. La crypto cherche à étaler un maximum le dictionnaire des termes alors que la compression cherche à faire l'inverse.

Les objectifs du stage sont entre autre les suivants

- Définition d'un algorithme offrant le meilleur compromis selon les contraintes suivantes
  - temps de cryptage,
  - résistance aux attaques,
  - volume de compression,
  - temps de compression
- L'algorithme doit également intégrer les contraintes suivantes
  - Décryptage partiel : les entités concernées par une plainte ne peuvent voir que leurs propres logs
  - Continuité : le système doit être stoppé en cas d'interférences dans le système d'écriture des logs
  - Complétude : on doit toujours travailler sur l'intégralité des activités

Réalisation et pré-requis

Le stage doit aboutir sur une maquette de démonstration intégrant l'algorithme spécifié. Le développement se fera en Scala ou Java sous OSGi, sur l'architecture LOGOS développée dans l'équipe Amazones.

Bibliographie

Liability in Software Engineering Overview of the LISE Approach and Illustration on a Case Study Le Métayer Daniel et Al. In *ACM/IEEE 32nd International Conf. on Software Engineering (ICSE 2010)*, May. 2, 2010, Cape Town, South Africa, pp. 135-144

Contact :
Laboratoire CITI, équipe Amazones
Stéphane Frénot
stephane.frenot@insa-lyon.fr

Cédric Lauradoux
Cedric.Lauradoux@inria.fr