Détection à base d'apprentissage automatique d'appels systèmes frauduleux dans les systèmes de type Unix

La cybersécurité est devenu aujourd'hui un enjeu majeur des systèmes informatiques. Les attaques potentielles sont nombreuses, que ce soit au niveau du réseau, des applications ou du système d'exploitation.

Ce dernier est l'élément le plus sensible d'un système informatique. Il est à la fois l'arbitre entre les différentes applications et/ou utilisateurs afin de garantir un partage et un accès équitable aux ressources, et le garant de la sécurité du système en vérifiant systématiquement que les processus ont les droits d'accès nécessaires à l'exécution des opérations (appels systèmes) qu'ils demandent.

À l'aide d'outils comme SystemTap [1], permettant d'instrumenter le noyau d'un système de type Linux, et Weka [2], qui implémente une grande variété d'algorithmes d'apprentissage automatique, l'objectif de ce projet est d'identifier quels seraient les algorithmes d'apprentissage les plus adaptés à une détection de tentative d'intrusion *via* les appels systèmes.

Le travail sera organisé de la façon suivante : 1) l'étudiant devra se familiariser avec la notion d'appel système et plus généralement l'interface entre les applications et le noyau du système d'exploitation et prendre en main l'outil SystemTap afin de l'instrumenter en vue de générer des traces caractéristiques d'appels systèmes ; 2) se familiariser avec Weka afin d'adapter les statistiques obtenues avec SystemTap au format requis par Weka ; 3) comparer la pertinence de plusieurs algorithmes fournis par Weka en vue de détecter une utilisation frauduleuse des appels systèmes par quelques commandes de base dy système.

References

[1] `https://sourceware.org/systemtap/`

[2] `https://www.cs.waikato.ac.nz/ml/weka/`

Contact

Éric Renault
ESIEE Paris – Université Gustave Eiffel
Bureau 5253
Email: `eric.renault@esiee.fr`
Tel: +33 1 45 92 60 78