Proposition de stage école d'ingénieur

Vérification de propriétés de sécurité par analyse statique

Mots-clés : méthode formelle, analyse statique, sécurité, Objective Caml.

Cadre

Le CEA LIST est un centre de recherche technologique sur les systèmes à logiciel prépondérant qui mène ses recherches en partenariat avec les grands acteurs industriels du nucléaire, de l'automobile, de l'aéronautique, de la défense et du médical pour étudier et développer des solutions innovantes adaptées à leurs besoins. Au sein du CEA LIST, le Laboratoire de Sûreté des Logiciels (LSL), localisé à Saclay (Essonne, 91), développe des outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels, tout particulièrement dans le domaine des systèmes embarqués critiques.

L'un des nos outils, nommé *Frama-C* (`http://frama-c.com`), est une plateforme logicielle facilitant le développement d'outils d'analyses statiques de programmes C. Le stage se déroulera au sein de l'équipe de R&D développant *Frama-C*, qui est programmé en *OCaml*.

Objectifs

Les programmes C contiennent de nombreuses sources de vulnérabilité, nuisibles à la sécurité générale du système car exploitables par des attaquants à des fins malicieuses. Ainsi, la bibliothèque standard du C contient un certain nombre de fonctions, comme `strcpy`, connues pour pouvoir être exploitées à de telles fins si elles sont appelées avec de mauvais arguments. De telles failles apparaissent aussi lorsque la séquence des appels à certaines fonctions n'est pas correcte (comme la séquences des appels à `malloc` et `free`, ou à `open` et `close`).

Le but du stage sera d'écrire une ou plusieurs analyses statiques légères sous la forme d'un greffon *Frama-C*, afin de détecter de telles erreurs de programmation potentiellement dangereuses pour la sécurité du système.

Le stage s'inscrit dans un projet plus large, dont le but est la vérification du programme *Bind* (`http://www.isc.org/software/bind/whatis`). Les vulnérabilités précises à détecter seront affinées en fonction de la durée du stage et du niveau du candidat.

Candidatures

Une maîtrise du langage *OCaml* est nécessaires pour ce stage. Posséder des notions d'analyse statique est un plus.

Contacts : Julien Signoles et Florent Kirchner (*prénom.nom*@cea.fr)

Les délais administratifs au CEA étant de 2 à 3 mois minimum, merci de prendre contact le plus tôt possible.