Proposition de stage

Étude de programmes C open-source avec un outil de vérification et analyse statique

Mots-clés : Méthodes formelles, vérification de programme, analyse statique, benchmarking, langage C

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 Sûreté et Sécurité des Logiciels (LSL), localisé à Nano-Innov (Palaiseau, 91), développe des outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels, tout particulièrement dans les domaines des systèmes embarqués critiques et de la cybersécurité.

L'un des nos outils, nommé *Frama-C* (`http://frama-c.com`), est une plate-forme logicielle facilitant le développement d'analyses de programmes C. Le stage se déroulera au sein de l'équipe développant *Frama-C*.

Objectifs

Le plug-in *Value* de la plate-forme Frama-C permet de vérifier l'absence d'erreurs à l'exécution dans un programme C donné. Ces erreurs peuvent amener à des *bugs*, comme des *crashes*, mais aussi à des vulnérabilités qui peuvent engendrer des failles de sécurité. Des méthodes de vérification sont couramment appliquées dans le domaine des systèmes embarqués critiques. Leur passage aux logiciels d'application plus générale requiert des développements pour gérer le fait que ces logiciels ont moins de contraintes lors de leur développement.

Le plug-in *Value*, originalement conçu pour le domaine de l'embarqué critique, évolue vers des applications plus générales (bibliothèques cryptographiques, utilitaires de ligne de commande, etc.), et cette évolution inclut des travaux pour le rendre plus facilement applicable sur de nouvelles études de cas (majoritairement, des bases de code *open-source*), ainsi que des évaluations de sa performance sur ces mêmes études.

Le stage comprendra plusieurs axes, d'importances variables en fonction des affinités de l'étudiant :

1. Identifier de nouvelles bases de code où le plug-in *Value* peut s'appliquer pour obtenir des résultats intéressants. Des exemples de constructions actuellement difficiles à analyser sont les appels récursifs et les structures telles que les listes chaînées, mais d'autres exemples pourraient être identifiés.
2. Effectuer le réglage du plug-in sur les études de cas identifiées, afin de trouver des erreurs à l'exécution potentielles, et minimiser le nombre de fausses alarmes ; idéalement, quelques faiblesses seront identifiées, et l'étudiant pourra donc suggérer des correctifs et améliorations à leurs développeurs ;
3. Classer les logiciels identifiés selon l'applicabilité du plug-in (par exemple : code cryptographique, utilitaire à la *Unix*, bibliothèque de communication réseau, etc.), en identifiant des caractéristiques qui permettront de prédire l'applicabilitié de l'outil sur une nouvelle base de code ;
4. Mesurer la performance, le taux de couverture et le nombre d'alarmes sur les études de cas, en fonction des réglages de l'outil. Cela permettra de tester son passage à l'échelle, ainsi que d'identifier ses limitations en termes de types de code.

Le stage permettra à l'étudiant de se familiariser avec les méthodes formelles et la vérification ; de bien connaître plusieurs aspects du langage C ; d'appliquer ses connaissances sur de vrais cas d'études ; et de contribuer à des améliorations sur des logiciels *open-source*.

Candidatures

Profil des candidats

- Intérêt pour la vérification de programmes
- Connaissance du langage C
- Capacité de travail en équipe
- La connaissance du langage *OCaml* est un plus, mais non requise

Conditions : stage indemnisé, aide au logement possible, transports CEA en Île-de-France.

Contact : André Maroneze, Boris Yakobowski (*andre.oliveiramaroneze@cea.fr*, *boris.yakobowski@cea.fr*)

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