Proposition de stage de BAC+5 Pro ou Recherche

Développement d'un outil de monitoring à base de simulation pour le code embarqué

Cadre du stage :

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 des Logiciels (LSL), localisé à Palaiseau (Essonne), développe les outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels.

L'un des nos outils, nommé Frama-C (http://frama-c.com), offre différents greffons pour l'analyse et la vérification de code C. Dans Frama-C, un programme C peut être annoté, c'est-à-dire, contenir des propriétés à vérifier exprimées par des annotations dans un langage de spécification formelle. Un des greffons de Frama-C, nommé E-ACSL, permet d'évaluer les annotations lors de l'exécution grâce à une instrumentation de code C, et de rapporter des échecs éventuels.

Un autre outil développé au LSL, UNISIM, offre une bibliothèque de simulation permettant de simuler sur un PC et de surveiller, à la manière des outils de débogage, l'exécution d'un code embarqué.

Objectifs du stage : La version existante du greffon E-ACSL effectue une instrumentation du programme C qui rajoute des variables et du code supplémentaires, ce qui n'est pas souhaitable dans un contexte contraint du code embarqué. Ce stage vise à développer un nouvel outil de monitoring et d'évaluation des annotations à l'exécution adapté aux contraintes du code embarqué. Il sera basé sur la simulation du code non-instrumenté à l'aide de la bibliothèque de simulation d'UNISIM.

La première étape du stage consistera à concevoir un protocole de communication avec une bibliothèque de simulation afin de pouvoir demander et transmettre les informations nécessaires pour évaluer les annotations (e.g. les valeurs des variables du programme). Ensuite, il faudra développer (en OCAML, dans un greffon de Frama-C) un outil de monitoring « à distance » qui fera des requêtes pour demander des informations nécessaires sur l'exécution simulée en utilisant le protocole défini, et réalisera l'évaluation des annotations. La version existante de E-ACSL pourra servir d'un point de départ pour cette implantation. Enfin, cet outil sera expérimenté sur des exemples de code embarqué.

Ce stage permettra au stagiaire de réaliser un outil de monitoring innovant, de l'appliquer à la vérification d'études de cas, et d'acquérir ainsi des compétences en vérification de code embarqué. Il existe des possibilités de continuer en thèse au CEA après le stage.

Profil des candidats :

- Bonne maîtrise des langages OCAML, C/C++.
- Connaissances en débogage et communication entre programmes souhaitées.
- Capacité de travail en équipe.

Conditions : stage indemnisé, aide au logement possible, transport CEA en Ile-de-France gratuit.

Encadrement : Nikolay Kosmatov, Gilles Mouchard, Julien Silgnoles.

Contact : Nikolay Kosmatov, email : nikolay.kosmatov@cea.fr

(Les délais administratifs au CEA étant assez longs, merci de nous contacter le plus tôt possible.)

Référence : M. Delahaye, N. Kosmatov, and J. Signoles. Common specification language for static and dynamic analysis of C programs. In SAC'13, pages 1230–1235, 2013.
http://kosmatov.perso.sfr.fr/nikolai/publications/delahaye_ks_sac_2013.pdf

Proposition de stage de BAC+5 Pro

Extension d'une bibliothèque de simulation pour le monitoring de la mémoire

Cadre du stage :

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 des Logiciels (LSL), localisé à Palaiseau (Essonne), développe les outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels.

L'un des nos outils, nommé Frama-C (http://frama-c.com), offre différents greffons pour l'analyse et la vérification de code C. Dans Frama-C, un programme C peut être annoté, c'est-à-dire, contenir des propriétés à vérifier exprimées par des annotations dans un langage de spécification formelle. Un des greffons de Frama-C, nommé E-ACSL, permet d'évaluer les annotations lors de l'exécution grâce à une instrumentation de code C, et de rapporter des échecs éventuels. Certaines de ces annotations portent sur des locations mémoires du programme (validité, initialisation, etc.).

Un autre outil développé au LSL, UNISIM, offre une bibliothèque de simulation permettant de simuler sur un PC et de surveiller, à la manière des outils de débogage, l'exécution d'un code embarqué. La version actuelle de la bibliothèque ne surveille pas spécifiquement la validité et l'initialisation des blocs mémoires dans l'exécution du programme simulé.

Objectifs du stage : La version existante du greffon E-ACSL effectue une instrumentation qui rajoute des variables et du code supplémentaires, ce qui n'est pas souhaitable dans un contexte très contraint du code embarqué. Dans le cadre d'un projet de développement d'un nouvel outil de monitoring et d'évaluation des annotations à l'exécution pour le code embarqué, ce stage vise à réaliser une extension de la bibliothèque de simulation d'UNISIM pour le monitoring avancé de la mémoire.

La première étape du stage consistera à identifier des moments dans l'exécution simulée et des informations qui doivent être signalées à l'outil de monitoring « à distance » afin de pouvoir mettre à jour le statut de la mémoire (allocation et libération des blocs mémoires, initialisation etc.). Ensuite, il faudra réaliser le transfert de ces informations vers l'outil de monitoring qui devra maintenir un modèle mémoire à jour afin de pouvoir évaluer les annotations sur l'état de la mémoire. Enfin, des expérimentations seront effectuées pour évaluer la solution développée.

Ce stage permettra au stagiaire de contribuer à la réalisation d'un outil de simulation et monitoring innovant, de l'évaluer sur des études de cas, et d'acquérir ainsi des compétences en simulation et vérification du code embarqué. Il existe des possibilités de continuer en thèse au CEA après le stage.

Profil des candidats :

- Bonne maîtrise des langages C et C++ et de la programmation bas niveau.
- Connaissances en débogage et communication entre programmes souhaitées.
- Capacité de travail en équipe.

Conditions : stage indemnisé, aide au logement possible, transport CEA en Ile-de-France gratuit.

Encadrement : Nikolay Kosmatov, Gilles Mouchard, Julien Silgnoles.

Contact : Nikolay Kosmatov, email : nikolay.kosmatov@cea.fr

(Les délais administratifs au CEA étant assez longs, merci de nous contacter le plus tôt possible.)

Référence : M. Delahaye, N. Kosmatov, and J. Signoles. Common specification language for static and dynamic analysis of C programs. In SAC'13, pages 1230–1235, 2013.
http://kosmatov.perso.sfr.fr/nikolai/publications/delahaye_ks_sac_2013.pdf

Proposition de stage de BAC+4 ou BAC+5 Pro ou Recherche

Vérification d'un micro-noyau sécurisé d'hyperviseur

Cadre du stage :

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 des Logiciels (LSL), localisé à Palaiseau (Essonne), développe les outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels.

L'un de ces outils, nommé Frama-C, permet de calculer les valeurs possibles des variables à chaque point de programme, trouver des menaces d'erreurs à l'exécution, prouver des propriétés du programme ou les vérifier à l'exécution, générer des cas de test, etc.

Un micro-noyau sécurisé pour une solution d'hypervision dite « en aveugle » a été développé par un autre laboratoire du CEA LIST. Il garantit la confidentialité et l'intégrité des données des machines virtuelles. Notamment, l'hyperviseur en aveugle n'a pas accès à la partition mémoire réservée pour une machine virtuelle car seul le micro-noyau sécurisé possède un contrôle total de la mémoire.

Objectifs du stage :

Ce stage vise à vérifier des algorithmes du micro-noyau sécurisé à l'aide des méthodes formelles (preuve de programmes, analyse de valeurs), de vérification à l'exécution et de test structurel en utilisant la plate-forme Frama-C. Un des composants critiques à vérifier est lié à la gestion de la mémoire.

Les algorithmes seront spécifiés et prouvés à l'aide des greffons de preuve de Frama-C. Des méthodes complémentaires (test, vérification à l'exécution) seront utilisées pour des fonctions qui ne seront pas entièrement prouvées.

Ce stage permettra au stagiaire de découvrir divers outils de vérification de logiciels et les technologies utilisées, les appliquer à la vérification d'un cas d'étude réel, et d'acquérir ainsi des compétences de plus en plus demandées par les entreprises. Il existe des possibilités de continuer en thèse au CEA après le stage.

Profil des candidats :

- Bonnes connaissances en génie logiciel, un goût pour les mathématiques et la logique.
- Langage C, notions en architecture et systèmes d'exploitation souhaités.
- Capacité de travail en équipe.

Conditions : stage indemnisé, aide au logement possible, transport CEA en Ile-de-France gratuit.

Encadrement : Nikolay Kosmatov

Contact : Nikolay Kosmatov, email : nikolay.kosmatov@cea.fr

(Les délais administratifs au CEA étant assez longs, merci de nous contacter le plus tôt possible.)

Références

[1] M, Aichouch and M. Ait Hmid. Towards an Implementation of a Blind Hypervisor. In : SEC2, https://sec2-2015.inria.fr/files/2015/06/aichouch-paper.pdf

[2] F.Kirchner, N.Kosmatov, V.Prevosto, J.Signoles, B.Yakobowski: Frama-C - A Software Analysis Perspective. Formal Asp. Comput. 27(3): 573-609 (2015) http://kosmatov.perso.sfr.fr/nikolai/publications/kirchner_kpsy_faoc_2015.pdf

Proposition de stage de BAC+4 ou BAC+5 Pro ou Recherche

Vérification d'un protocole de communication de réseau de capteurs à l'aide d'outils de vérification automatique

Cadre du stage :

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), développe les outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels.

L'un de ces outils, nommé Frama-C, permet de calculer les valeurs possibles des variables à chaque point de programme, trouver des menaces d'erreurs à l'exécution, prouver des propriétés du programme ou les vérifier à l'exécution, générer des cas de test, etc.

Dans le cadre d'un projet collaboratif, le CEA LIST travaille sur l'implémentation et la validation de protocoles de réseaux de capteurs qui seront utilisés dans des domaines critiques (avionique, transport, etc.)

Objectifs du stage :

Ce stage vise à vérifier des logiciels embarqués dans un réseau de capteurs à l'aide des outils de vérification automatique. Dans un premier temps, il s'agira d'identifier et de spécifier des propriétés de sûreté et sécurité de fonctionnement, notamment, liées à la communication et diffusion de messages. Ces propriétés seront ensuite spécifiées dans le langage de spécification de la plate-forme Frama-C, incluant des preconditions, postconditions, assertions, etc. Ensuite, des outils de vérification seront appliqués pour vérifier les propriétés spécifiés et identifier des éventuelles erreurs.

Les algorithmes seront spécifiés et ensuite prouvés à l'aide des greffons de preuve de Frama-C. Le prototype développé au CEA LIST sera utilisé comme le point de départ des travaux. Les techniques de test ou vérification à l'exécution pourront être utilisées pour la validation des parties du code qui ne pourront pas être entièrement prouvées. Ce stage permettra au stagiaire de découvrir divers outils de vérification de logiciels et les technologies utilisées pour assurer la sûreté et la sécurité de logiciels, les appliquer à la vérification d'un cas d'étude réel, et d'acquérir ainsi des compétences de plus en plus demandées par les entreprises. Il existe des possibilités de continuer en thèse au CEA après le stage.

Profil des candidats :

- Des connaissances en génie logiciel, un goût pour les mathématiques et la logique.
- Bonnes connaissances du langage C, notions en protocoles de communication souhaitées.
- Capacité de travail en équipe.

Conditions : stage indemnisé, aide au logement possible, transport CEA en Ile-de-France gratuit.

Encadrement : Nikolay Kosmatov, email : nikolay.kosmatov@cea.fr

(Les délais administratifs au CEA étant assez longs, merci de nous contacter le plus tôt possible.)

Références

[1] F.Kirchner, N.Kosmatov, V.Prevosto, J.Signoles, B.Yakobowski: Frama-C - A Software Analysis Perspective. Formal Asp. Comput. 27(3): 573-609 (2015)
http://kosmatov.perso.sfr.fr/nikolai/publications/kirchner_kpsy_faoc_2015.pdf