

Détection automatique de faiblesses de sécurité dans du code C et C++

Thématique : sécurité de logiciel, système embarqué, compilation, algorithmique

Lieu: MathWorks. 38330 Montbonnot Saint-Martin (près de Grenoble)

Dépôt de Candidature : <http://www.mathworks.com/company/jobs/opportunities> Search Jobs
FR-Grenoble

Durée de stage : 6 mois

Rémunération aux alentours de 1000 euros bruts / mois (selon formation)

Polyspace (<http://www.mathworks.com/products/polyspace/index.html>) est un outil de validation statique de programmes développé par la société MathWorks. Polyspace Code Prover permet de prouver mathématiquement l'absence de certaines erreurs à l'exécution sur les programmes écrits en langage Ada, C et C++. Polyspace Bug Finder permet de détecter un grand nombre d'erreurs rapidement sur des applications de grande taille écrites en C et C++. Ces deux produits sont largement utilisés dans les secteurs de l'informatique embarquée : automobile, aéronautique, transports et nucléaire.

Les faiblesses de sécurité deviennent aujourd'hui un problème central dans beaucoup de systèmes embarqués. Polyspace Bug Finder a pour vocation d'adresser ce problème spécifique. L'objectif du stage est de participer à l'amélioration de cette fonctionnalité.

Un prérequis du stage est d'être un minimum familier avec les thèmes de sécurité de logiciel en général, familier avec le langage C/C++ et intéressé par les aspects de compilation.

Entre autres, le stagiaire devra au cours du stage :

- Dresser une liste de fonctions standards réputées problématiques mais largement utilisées sur Unix/Linux et Windows ;
- Approfondir ses connaissances sur les aspects d'authentification, de cryptographie, et de certification ;
- Modéliser la reconnaissance automatique de présence/absence de séquences de patterns sur la représentation interne du compilateur de Polyspace ;
- Réaliser un prototype basé sur les techniques de compilateurs ou d'autres techniques pour évaluer l'efficacité de ces modèles sur un sous-ensemble des défauts répertoriés.