Proposition de stage niveau bac+5

Compatibilité de Frama-C aux vulnérabilités du CWE

Mots-clés : analyse statique, vulnérabilités, spécification formelle, OCAML

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 (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, *Frama-C* (`http://frama-c.com`), est une plate-forme logicielle facilitant le développement d'outils d'analyses de programmes C. Ces outils servent à l'analyse de la fiabilité et de la sécurite de programmes C. Le stage se déroulera au CEA LIST dans l'équipe de R&D développant *Frama-C*.

Objectifs

L'objectif de ce stage est de rendre *Frama-C* compatible aux CWE, (Common Weakness Enumerations), `https://cwe.mitre.org`, de préparer un dossier de soumission et de soumettre celui-ci afin d'obtenir le certificat de compatibilité.

Depuis quelques années, les outils d'analyse de programmes C sont capables d'analyser non seulement la fiabilité mais également la sécurité au niveau du code C. Pour l'outil *Frama-C* divers composants ont été developpés afin de détecter le respect de propriétés de sécurité, au travers de projets de recherche européens et nationaux. En matière de sécurité logicielle, les CWE font référence pour classifier les vulnérabilités. Pour chacune d'elles, ils fournissent une description détaillée, le niveau de sévérité, les langages de programmation et le système d'exploitation impactés, les mitigations possibles, une taxonomie et un historique.

MITRE Corp. a initié un programme de compatibilité (`https://cwe.mitre.org/compatible/declare.html`) permettant aux outils d'analyse de code d'être estampillés "compatibles aux CWE". Un tel outil doit pour cela fournir un certain nombre de fonctionnalités permettant de l'employer pour la détection de vulnérabilités :

- capacité de détecter des occurrences de vulnérabilités et de les présenter dans la numérotation officielle CWE
- capacité de rechercher des occurrences de vulnérabilités spécifiées
- capacité de documenter précisement la compatibilité avec la classification CWE
- capacité de décrire précisement la couverture exacte des vulnérabilités détectées
- publier les capacités de détection de vulnérabilités de la classification.

Afin de rendre *Frama-C* compatible à CWE, il faut développer un plug-in pour *Frama-C* remplissant les fonctionnalités exigées ci-dessus et s'appuyant sur les plug-ins d'analyse existants de *Frama-C*.

Pour cela, les travaux suivants seront à réaliser :

- **Tâche 1 :** L'outil *Frama-C* n'étant capable que de détecter des anomalies au niveau du code source C et C++, il s'agit de déterminer le périmètre des vulnérabilités détectables à ce niveau. On partira de la liste déja établie par le projet Européen FP7 STANCE (livrable D1.4 fourni).
- **Tâche 2 :** développement d'un plug-in d'interface, traduisant les warnings générés par le plug-in d'interprétation abstraite de *Frama-C* en warnings au format CWE. Un IHM sera à developper pour ce nouveau plug-in.
- **Tâche 3 :** certaines vulnérabilités de la liste ne sont pas couvertes par aucun composant actuel de *Frama-C*, on déterminera lesquelles sont détectables par *Frama-C* moyennant des développements additionnels.
- **Tâche 4 :** Développement de composants nouveaux pour la détection de vulnérabilités restantes déterminés dans la tache 3.
- **Tâche 5 :** Aide a la constitution du dossier de soumission au programme de compatibilité CWE et soumission en ligne sur le site web MITRE.

Durée du stage : 6 mois.

Références

Candidatures

La maîtrise des langages C et *OCaml* est nécessaire pour ce stage. Des connaissances en C++ et en analyse de programmes sont des atouts.

Contacts : Julien Signoles, Virgile Prevosto, Armand Puccetti (`prenom.nom@cea.fr`)

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