THALES

Offre de stage

Couverture de code à l'aide de fuzzing et d'exécution symbolique

Situation organisationnelle : Thales Research & Technology France

Dir./Dépt. : STI

Service : LSEC

Personnes à contacter : Nikolaï KOSMATOV – nikolai.kosmatov@thalesgroup.com,

Delphine Longuet delphine.longuet@thalesgroup.com

Durée du stage : 6 mois

A pourvoir : à partir de Janvier 2021

Lieu : Palaiseau, France

Description du contexte :

Le Groupe de Recherche Logiciel de TRT-Fr se compose de plusieurs laboratoires dont un est spécialisé dans la conception des systèmes temps-réel embarqué critiques (LSEC).

THALES conçoit et développe des systèmes temps-réel de plus en complexes et critiques. De ce fait, la difficulté de validation et de vérification de ces systèmes est croissante. Lors de la validation des logiciels faisant partie de ces systèmes, on cherche généralement à atteindre une couverture élevée du programme sous test, c'est-à-dire, créer une suite de test qui activent les différentes parties du programmes (les instructions, les branches, les chemins, etc.). Cela permet de valider le système avec un niveau de confiance élevé. Dans certains domaines critiques, une couverture rigoureuse du programme fait également partie des exigences imposées par des normes de certification.

Les outils de génération automatique de tests à base d'exécution symbolique (e.g. PathCrawler, KLEE, Java PathFinder, etc.) peuvent permettre de générer des tests pour une couverture de test, mais rencontrent des limitations au niveau des performances et des capacités de traiter des codes complexes. D'autre part, les outils de fuzzing (e.g. AFL, AFL++, Eclipser, etc.) permettent de générer un grand nombre de données de test rapidement et pour tout type de code, mais ne sont pas toujours capables d'assurer un niveau de couverture élevé.

Ce stage propose d'étudier les possibilités de combinaisons des outils d'exécution symbolique et de fuzzing, de proposer des techniques et méthodologies d'utilisations optimisées pour atteindre une couverture de code augmentée, et de les évaluer sur des benchmarks. On s'intéressera également à la couverture d'un ensemble d'objectifs de couverture (notamment, pertinent pour la cybersécurité) pour évaluer l'apport des techniques proposées pour la détection de vulnérabilités potentielles dans le code.

Vos missions et objectifs du stage :

Les activités de ce stage seront de :

1. Réaliser un état de l'art complémentaire des outils de génération de tests et de fuzzing les plus récents (pour compléter l'état de l'art et l'évaluation effectués précédemment) ;
2. Evaluer une sélection d'outils sur des benchmarks en cherchant à identifier les limites des différents outils et de créer une base de codes pour évaluation ;
3. Proposer des techniques et méthodologies combinant les différentes approches ;
4. Evaluer les techniques proposées sur des programmes identifiés et des codes open-source disponibles par rapport à la couverture.
5. Evaluer l'impact des combinaisons proposées pour les propriétés de cybersécurité.

Votre profil: Master Recherche ou Pro d'Informatique ou Ecole d'ingénieurs, spécialité Génie Logiciel ou équivalente
Niveau d'étude : Bac+5 (Master 2 ou Diplôme d'ingénieur)
Connaissances indispensables : Un ou plusieurs des langages : C/C++, Java, Ada. Génie logiciel. Test de logiciels.
Connaissances souhaitables : Méthodes formelles, Analyse de programme.
Langues : français, anglais