Soutenance de thèse

Viet Hoang LE soutiendra sa thèse de doctorat, préparée au sein de l'équipe d'accueil doctoral ISAE-ONERA MOIS et intitulée «*Une couverture combinant tests et preuves pour la vérification formelle*»

Le 11 juillet 2019 à 14h00,
Bâtiment hexagonal de l'ONERA - 2 Avenue Edouard Belin, 31000 Toulouse

devant le jury composé de

Mme Virginie WIELS	Directrice de Recherche ONERA/DTIS	Directrice de thèse
M. Julien SIGNOLES	Ingénieur de Recherche CEA List/LSL	Co-directeur de thèse
Mme Catherine DUBOIS	Professeure ENSIIE	Rapporteur
M. Ioannis PARISSIS	Professeur Grenoble INP	Rapporteur
Mme Hélène WAESELYNCK	Directrice de Recherche LAAS-CNRS	
Mme Delphine LONGUET	Ingénieure de Recherche Thales Research & Technology	

Résumé :

Actuellement, le développement d'un logiciel de taille industriel repose généralement sur des tests ou des preuves unitaires pour garantir rigoureusement ses exigences. En outre, il a déjà été montré que l'utilisation combinée du test et de la preuve unitaires est plus efficace que l'utilisation d'une seule de ces deux techniques. Néanmoins, un ingénieur en vérification hésite encore à utiliser ces deux techniques conjointement, faute d'une notion de couverture commune au test et à la preuve. Définir une telle notion est l'objet de cette thèse. En effet, nous introduisons une nouvelle couverture, appelée « couverture label-mutant ». Elle permet de représenter les critères de couverture structurelle habituels du test, comme la couverture des instructions, la couverture des branches ou la couverture MC/DC et de décider si le critère choisi est satisfait en utilisant une technique de vérification formelle, qu'elle soit par test, par preuve ou par une combinaison des deux. Elle permet également de représenter les critères de couverture fonctionnelle. Nous introduisons aussi dans cette thèse une méthode reposant sur des outils automatiques de test et de preuve pour réduire l'effort de vérification tout en satisfaisant le critère de couverture choisi. Cette méthode est mise en oeuvre au sein de la plateforme d'analyse de code C (Frama-C), fournissant ainsi à un ingénieur un moyen opérationnel pour contrôler et réaliser la vérification qu'il souhaite.

Mots-clés : vérification de programmes, test unitaire, preuve de programmes, combinaison d'analyse, couverture de code

Summary: The objective is to study the combination of static and dynamic techniques for the verification of safety properties, leaving as open as possible the type of combination envisaged. For this, two axes can be explored. On the one hand, at the methodological level, it will be possible to study how to formalize a security property expressed at model level or a system into a set of properties of lower level at application level and verifiable by static analysis tools or dynamic analysis tools. On the other hand, at the program analysis level, it will be possible to investigate how to combine in practice different existing static and dynamic analyzers to check a set of properties expressing a higher level of security property.

Keywords: program verification, unit testing, program proving, analysis combination, code coverage