Avis de Soutenance

Monsieur Yani ZIANI

Informatique

Soutiendra publiquement ses travaux de thèse intitulés

Vérification formelle de couches de confiance dans les logiciels : application à la TPM Software Stack

dirigés par Monsieur Frederic LOULERGUE et Monsieur Nikolay KOSMATOV
Ecole doctorale : Mathématiques, Informatique, Physique Théorique et Ingénierie des Systèmes - MIPTIS
Unité de recherche : LIFO - Laboratoire d'Informatique Fondamentale d'Orléans

Soutenance prévue le ***jeudi 09 octobre 2025*** à 14h00
Lieu : Thales Research & Technology 1 Avenue Augustin Fresnel, 91120 Palaiseau
Salle : Auditorium

Composition du jury proposé

M. Frédéric LOULERGUE	Université d'Orléans	Directeur de thèse
Mme Catherine DUBOIS	ENSIIE (École Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise)	Rapporteure
M. Alain GIORGETTI	Université Marie et Louis Pasteur/Institut FEMTO-ST UMR CNRS 6174	Rapporteur
M. Nikolai KOSMATOV	Thales Research & Technology	Co-directeur de thèse
M. Wolfgang AHRENDT	Chalmers University of Technology	Examinateur
M. Claude MARCHé	INRIA Saclay - Île-de-France	Examinateur
M. Mickael DELAHAYE	Direction Générale des Armées	Invité
M. Daniel GRACIA PEREZ	Thales Research & Technology	Invité

Mots-clés : méthodes formelles,vérification déductive,vérification dynamique,Frama-C,TPM software stack,

Résumé :

Le Trusted Platform Module (TPM) est un cryptoprocesseur conçu pour protéger l'intégrité et la sécurité des ordinateurs modernes. Les communications avec le TPM passent par la TPM Software Stack (TSS), qui joue le rôle de couche de confiance pour le TPM. La bibliothèque open-source tpm2-tss (écrite en C) est une implémentation largement utilisée de la TSS. Actuellement, la spécification et la vérification d'applications critiques pour la sécurité telles que la librairie tpm2-tss restent un défi important, en particulier lorsque le code n'est pas écrit dans l'optique d'être vérifié. L'objectif de cette thèse est d'explorer dans quelle mesure il est actuellement possible de spécifier et de vérifier des propriétés de sécurité, des propriétés fonctionnelles et des propriétés de sûreté sur un code critique qui n'a pas été pensé pour la vérification. La plateforme de vérification Frama-C et certains de ses principaux analyseurs (Wp, E-ACSL et MetAcsl) sont utilisés pour étudier l'efficacité de diverses techniques de vérification dans ce contexte. En ce qui concerne la vérification déductive à l'aide de Wp, la spécification et la vérification de propriétés fonctionnelles et de l'absence d'erreurs à l'exécution sur un sous-ensemble représentatif de fonctions mettent en évidence plusieurs limitations et des solutions de contournement nécessaires, notamment lorsqu'il s'agit d'allocations dynamiques et de structures de données récursives. Par ailleurs, lorsque la vérification déductive s'avère

difficile à appliquer à ce type de code, l'outil de vérification à l'exécution E-ACSL est utilisé pour vérifier les propriétés de sécurité de haut niveau écrites avec MetAcsl. Cette approche offre un moyen plus accessible d'évaluer des propriétés de haut niveau sur des programmes de grande taille, mais donne moins de confiance dans les résultats de la vérification. Enfin, nous explorons des approches combinées pour évaluer les propriétés de tels programmes : d'abord en combinant la vérification déductive avec l'analyse de forme fournie par l'outil MemCAD pour se concentrer sur les propriétés de bas niveau; ensuite en combinant Wp et E-ACSL pour la vérification d'exigences de haut niveau écrites avec MetAcsl.