Offre de stage

Chaîne open-source pour la vérification de programmes C

Encadrants Emmanuelle Encrenaz-Tiphene, Dylan Marinho

Laboratoire LIP6, CNRS UMR 7606, Sorbonne Université

Équipe
- ALSOC (Architecture et Logiciels pour Systèmes Embarqués sur Puce) ,
- MoVe (Modélisation et Vérification)

Keywords méthodes formelles · systèmes paramétrés · model checking · logiques temporelles · automates temporisés

1. Contexte

Les systèmes temps réel interviennent dans des domaines critiques (transports, télécommunications, systèmes embarqués industriels) et doivent satisfaire des contraintes temporelles strictes. La preuve formelle du respect de ces contraintes et de propriétés de sécurité associées est un enjeu majeur pour la fiabilité et la sûreté des systèmes.

Ce projet porte sur la vérification de propriétés de sécurité fondées sur des observations temporelles. En particulier, une fuite temporelle se produit lorsqu'un adversaire, en observant des durées d'exécution ou des dates d'événements, peut déduire des informations sensibles sur l'état interne du système.

Nous nous focalisons sur la notion d'opacité — une propriété de sécurité qui formalise l'impossibilité pour un attaquant de distinguer des exécutions "secrètes" d'exécutions "non secrètes" à partir des seules observations disponibles. Dans des travaux antérieurs, nous avons défini et étudié l'opacité par rapport au temps d'exécution (ET-opacity) ([And+22] ; [And+23] pour un aperçu plus récent).

Par ailleurs, [And+25] propose une chaîne de traduction automatisée de programmes C vers des modèles exploitables par le model-checker Roméo. Cette chaîne est disponible en *open-source* sur GitHub.

Le présent stage vise à poursuivre et renforcer ces travaux en :
- étendant l'outil existant pour supporter un sous-ensemble plus riche du langage C ;
- intégrant une modélisation du cache de données afin de capturer des fuites temporelles liées au comportement mémoire.

2. Objectifs du stage

Ce stage se décline autour de trois objectifs :

- Extension de la chaîne de traduction : renforcer l'outil existant pour supporter un sous-ensemble élargi d'instructions afin de faciliter la traduction de la bibliothèque STAC étudiée dans [And+25] ainsi que d'exemples d'autres bibliothèques.
- Portage et validation d'exemples STAC : traduire des exemples issus de la librairie STAC (initialement en Java) vers des programmes C, puis valider leurs résultats à l'aide de Roméo.
- Modélisation du cache de données : proposer et implémenter une abstraction réaliste du cache de données.

3. Compétences

Les compétences suivantes ne sont pas obligatoires, mais seraient les bienvenues :
- model checking
- automates/réseaux de Petri temporisés (paramétrés)
- programmation (en C et en Java)
- notions d'architecture matérielle (cache, mémoire)

4. Conditions

Le stage aura lieu au LIP6, au sein de Sorbonne Université à Paris. Le LIP6 est une unité mixte de recherche (UMR 7606) de Sorbonne Université (SU) et du Centre national de la recherche scientifique (CNRS). C'est un laboratoire de recherche en informatique comptant environ 450 membres, dont plus de 170 chercheurs permanents.

Candidature : par email.

References

[And+22] Étienne André, Didier Lime, Dylan Marinho, and Sun Jun, "Guaranteeing timed opacity using parametric timed model checking," *ACM Transactions on Software Engineering and Methodology*, vol. 31, no. 4, pp. 64:1–64:36, 2022, doi: 10.1145/3502851.

[And+23] Étienne André, Engel Lefaucheux, Didier Lime, Dylan Marinho, and Sun Jun, "Configuring Timing Parameters to Ensure Execution-Time Opacity in Timed Automata," in *TiCSA@ETAPS 2023*, 2023, pp. 1–26. doi: 10.4204/EPTCS.392.1.

[And+25] Étienne André *et al.*, "Verifying Timed Properties of Programs in IoT nodes using Parametric Time Petri Nets," in *SAC 2025*, 2025, pp. 1998–2006. doi: 10.1145/3672608.3707861.

CNRS · LIP6 4 place Jussieu · 75005 Paris
✉ Dylan.Marinho@sorbonne-universite.fr 💻 perso.lip6.fr/Dylan.Marinho