Université de Rennes

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2025

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : Matisse **POLE DE RECHERCHE :Mathématiques-Numérique**

Unité de recherche d'accueil

Unité de Recherche : Irisa

Equipe : EPICURE

Encadrement

Directeur de thèse : Thomas Jensen **Unité de recherche** : Irisa

Employeur/Établissement d'origine :Inria

HDR : • oui **Nb de thèses en cours** : 3

Mail : thomas.jensen@irisa.fr **Tél**. :(+33 / 0) 2 99 84 74 78

Co-directeur de thèse : **Unité de recherche** :

Employeur/Établissement d'origine :

HDR : • oui • non **Nb de thèses en cours** :

Mail : **Tél.** :

Sujet

Titre : Formal Verification of Root of Trust Software

Mots clés : Formal Verification, Security, End-to-End mechanised proof

Cotutelle internationale (oui/non) : **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :

The security of software systems is based on a chain of trust that is rooted in the hardware and ensures the security, in particular the integrity of computations run in higher layers of abstractions e.g. user code running on an operating system. Therefore, the root of trust (RoT) is a critical piece of software that is run when a device is powered up and any vulnerability in this code is compromising the security of any other code running on the device. One of the key propertyof the RoT is to verify the integrity of software running on the device. For instance, a secure boot verified that the code operating system has not been tampered with.

The thesis will investigate the formal verification of RoT software. Compared to other software RoT have are several distinctive features that make their verification a challenge.
- A first challenge is the tight cooperation of the RoT software with security features of the hardware e.g. cryptographic keys sealed in the silicium. To be adequate, the formal model needs to provide a fine-grained model of the hardware which goes beyond the classic Instruction Set Architecture.
- Another challenge is that the software is typically written using both C code and assembly code for which semantics model are either missing or difficult to reason with.

Typically, there is a verification gap between a formal model and the running software. The thesis will tackle the challenge of verifying RoT software with the objective of narrowing the verification gap to the minimum.

To get to this objective, the thesis will investigate how to adapt the techniques coming from verified compilation to automatically extract from the formal model an executable code that can be used as an in-place replacement. As RoT software cannot rely on any platform service or runtime this changes the focus compared to existing approaches to compile specification to executable code. To assess the developed techniques, the thesis will consider case-studies with features highlighting the difficulties of RoT software and showing that the proposed solution are adequate.

w

Université de Rennes

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2025

Contrats doctoraux «Ordinaires»

➢ **Ce document est à renvoyer par la direction de l'unité de Recherche aux animateurs du Pole Recherche et à l'école Doctorale pour le 13 février 2025 au plus tard**