Formal verification of hardware specifications

Guillaume Hiet, Pierre Wilke
CIDRE, CentraleSupélec

Thomas Letan
Formal methods expert in Laboratoire de Sécurité du Logiciel at ANSSI

Context. Formal methods have been successfully applied to software in the last decades. In particular, CompCert [1] is a formally verified compiler for C, where the source C program and the compiler assembly program are proved to be equivalent; or the static analyser Astrée [2], which shows the absence of run-time errors in C programs.

These works are based on a model of the machine on which programs will be executed. In order to extend the formal guarantees given by tools like CompCert or Astrée to actual runs of programs on a machine, one has to bridge the gap between the model used for verification and the actual hardware. This is the direction we propose to explore in this internship.

There are already some work in that direction. Reid [4] proposes a formal specification of the ARM architecture. For instance, Kami [3] is a library written in Coq [5] which allows to specify, implement and verify hardware designs down to FPGA circuits. As an application of their framework, they build a formal model of a RISC-V processor. SpecCert [6] is another framework that aims at modular modelling of complex systems and verification of security policies.

Objectives. Our long-term goal is to apply formal methods to complex architectures of hardware devices, in order to verify security properties such as component isolation and integrity. Depending on the student’s preferences, the internship could focus on one of the following aspects:

- Bridge the gap between the RISC-V models used in CompCert and Kami. More precisely, CompCert gives a formal semantics of the RISC-V Instruction Set Architecture (ISA) and the RISC-V Kami model gives another one. The goal is therefore to verify that these two models agree on a common semantics. This would allow to establish an
end-to-end formal guarantee from C source files to actual hardware implementations.

- **Ensure the security of hardware components.** Given a security policy, the goal would be to prove that this security policy is indeed enforced by security mechanisms present in the architecture. For instance, we could focus on the ring mechanisms that discriminate kernel and user modes, and prove isolation properties. The methodology used in SpecCert [6] could be adapted to operate on the existing RISC-V model in Kami.

**Profile.** The interested student should be familiar with the Coq proof assistant (having attended the SEM course, for instance), and have an interest in hardware architecture and security.

**Contact.**

- Guillaume Hiet guillaume.hiet@centralesupelec.fr
- Pierre Wilke pierre.wilke@centralesupelec.fr

**Keywords.** formal methods, hardware architecture, security policy.

**References**


