Short-Term Scientific Mission Grant
- APPLICATION FORM[1] -

Action number: CA20111

Applicant name: Volker STOLZ

Details of the STSM

Title: **Coupling SMT and theorem proving to prove hardware/software security mechanisms**

Start and end date: 01/09/2024 to 11/09/2024

Goals of the STSM

Theorem provers allow an encoding of important operational properties of systems in an unequivocal manner. Our topic of interest are security and tracing mechanisms at the lower level of IT architecture. Semi-formal specifications describe the data format and its interpretation. This data is used to make important assessments of the health of a system, e.g. to identify attack attempts. It is therefore important that the mechanisms are adequately captured and can be subjected to formal analysis of implemented and intended behaviour.

We combine our expertise in semantics and static analysis (Stolz) with the experience in cybersecurity and low-level hardware features (Hiet) and build on the recent advances and contribute to WG3 Program Verification of the COST Action by investigating the combination of SAT/SMT-based techniques and theorem proving.

Working Plan

During the visit, we make use of the specialised hardware (ARM-based SoCs) available at the STSM's host's institution to use the low-level processor trace mechanism to obtain execution traces of sample programs, and their concrete experience on this platform.

These traces are in a highly compressed binary format. Open-source trace decoders exist e.g. in C++, but are not amenable to an analysis of their correctness. We will investigate the feasibility of reformulating a decoder in OCaml & Coq and guarantee its correctness. Due to the necessary handling of binary data, we will in particular study the use of SMTCoq to increase automation in proofs (M. Armand, G. Faure, B. Grégoire, C. Keller, L. Théry, B. Werner: "A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses", CPP 2011).

Decoded traces can be used in monitoring security properties of running applications. During the visit, we will look into connecting the security properties of example applications with their respective permitted traces and a (usually state-machine driven) monitoring mechanism, building on the expertise in HIET's

[1] This form is part of the application for a grant to visit a host organisation located in a different country than the country of affiliation. It is submitted to the COST Action MC via e-COST. The Grant Awarding Coordinator coordinates the evaluation on behalf of the Action MC and informs the Grant Holder of the result of the evaluation for issuing the Grant Letter.

group (M. Baty, P. Wilke, G. Hiet, A. Fontaine, A. Trieu: “A Generic Framework to Develop and Verify Security Mechanisms at the Microarchitectural Level: Application to Control-Flow Integrity”, CSF 2023).

The invitee will meet with the research group members in Rennes (Hiet, Baty, Wilke) and plan future collaboration on the experimental results that we have obtained and how to collaborate remotely.

Expected outputs and contribution to the Action MoU objectives and deliverables.

Main expected results and their contribution to the progress towards the Action objectives (either research coordination and/or capacity building objectives) and deliverables.

Our STSM contributes to the following objectives:

We aim to make progress in the state-of-the-art for verifying properties on the lower levels of the architecture such as trace decoders, and provide useful abstractions, their formalization in the Coq theorem prover, and proofs of their properties (O-R3: Make techniques for program verification more effective and more accessible to all stakeholders).

We aim to publish our machine-readable contributions in open repositories and ultimately publish our results and serve as input to a potential submission to EU Horizon calls in that domain (O-C2: Act as a stakeholder platform in the field of formal proofs from its theoretical grounds to its industrial applications, O-C8: Disseminate the results of the Action activities to the scientific community, the industry, the certification bodies, the European institutions and to the general public).

We hope to achieve this by combining the expertise of STOLZ in formalizing semantics with HIET’s expertise in security- and hardware properties (O-C1: Bring together members of the different communities working on proofs in Europe).

In particular, our STSM contributes to the aims of WG3 on Program Verification: we capture the complexity of low-level hardware features and make them amenable techniques for the verification of program correctness, and jointly investigate the applicability of recent synergies between SAT/SMT-solving and theorem proving, and how it can be harnessed it in our domains. The outcomes will be referenced from the WG git repository.

The standard internal funding for research-activities at HVL is currently 15.000 NOK (ca. 1.300 EUR) per academic year per faculty member. This creates severe constraints on the academic activities such as research visits and conference participation. Funding by the COST Action would give us a possibility to look into this very interesting topic and enable future collaboration.