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

Action number: CA20111

Applicant name: Muhammad Usama Sardar

Details of the STSM

Title: Formal Specification and Verification of Attestation in Confidential Computing

Start and end date: 14/05/2023 to 20/05/2023

Goals of the STSM

Purpose and summary of the STSM.

(max.200 word)

I as well as the host Dr. Lilia Georgieva participated in the recent WG3 meeting in Timisoara and this is a follow-up. The aim is to compare various approaches for formal specification and verification in the context of attestation protocols in confidential computing for WG3 deliverable D5 (month 18): Comparison of the approaches used in the Software Verification competition SV-COMP. We envision progressing from the security (in contrast to the safety) perspective of program verification. More specifically, we plan to analyze and characterize approaches and tools in symbolic protocol verification from a practical perspective for challenging contexts, such as an attacker with root access to the system (such as public cloud where the program is deployed).

Working Plan

Description of the work to be carried out by the applicant.

(max.500 word)

At the host university (Heriot-Watt University) and neighbouring institutions (the University of Edinburgh and the University of Stirling), I will give a talk on the state-of-the-art work (joint work in collaboration with industrial partners at Arm Ltd.) on verification of attestation protocols in confidential computing [1]. Modern systems use Confidential Computing techniques to protect data, code and secrets. In the proposed talk, we share our experiences using ProVerif tool, where we discovered several design and security flaws in the state-of-the-art Confidential Computing solutions. In this context, one of the goals is to make the verification approaches and tools more accessible to systems engineers so these tools can be used for effective and secure design.

I will then discuss with the host Dr. Lilia Georgieva and her research group work about their work on using SPIN model checker, model analyzer Alloy, and AVISPA tool for security verification. We will explore and summarize tools for verification of security properties, such as what kind of properties can be verified and any limitations on modeling and verification.

[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.

Funded by
the European Union

We will also discuss possibilities of collaboration for topics of mutual interest.

[1] https://www.researchgate.net/publication/367284929_SoK_Attestation_in_Confidential_Computing

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.

(max.500 words)

This STSM contributes to the WG3 deliverable D5's output 3: Applications: formal specification and verification of security protocols in emerging and challenging contexts (such as attestation in Confidential Computing) as discussed in WG3 meeting in Timisoara [1].

[1] https://europroofnet.github.io/_pages/WG3/Feb2023/ReportWG3TimisoaraMeeting.pdf