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: 10/09/2023 to 14/09/2023

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 WG3 meeting in Timisoara in February and had a STSM in May for WG3 deliverable D5 (month 18): Comparison of the approaches used in the Software Verification competition SV-COMP. More specifically, the STSM contributed to output 3 of deliverable D5 namely Applications: formal specification and verification of security protocols in emerging and challenging contexts (such as attestation in Confidential Computing). During STSM, we explored the comparison of formal specification of security-relevant properties using different tools in symbolic protocol verification, and compiled a 7-page draft for the deliverable. This STSM is a follow-up to have some focused time to refine and finalize the report for deliverable D5.

Working Plan

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

(max.500 word)

I will further 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, and see how these tools can provide additional insights compared to our approach based on ProVerif. We will continue discussion on the comparison of tools, and refine and finalize the report for deliverable D5.

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.

[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.

(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