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

Action number: CA20111

Applicant name: Muhammad Usama Sardar

Details of the STSM

Title: Challenges in the Formal Verification of Attested TLS in Confidential Computing

Start and end date: 09/06/2024 to 15/06/2024

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 2023 and had a STSM in May 2023 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 extend the draft with our latest research on attested TLS, i.e., integrating attestation in Transport Layer Security (TLS) protocol.

Working Plan

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

(max.500 word)

I will continue discussion with the host Dr. Lilia Georgieva and her research group 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 extend the draft created in the previous STSM for submission as a survey paper.

During the STSM, we will present our survey so far to seek feedback at the host university (Heriot-Watt University) and the University of Stirling (hosts: Dr. Patrick Maier and Dr. Wen shin Lee), and industrial

[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.

partners (Microsoft Azure for Operators (AFO) Research and Arm).

The work plan is structured as follows:

Day 1-2: Presentation and discussion with the host Dr. Lilia Georgieva at Heriot-Watt University

Day 3: Presentation and discussion with the hosts Dr. Patrick Maier and Dr. Wen shin Lee at University of Stirling

Day 4: Presentation and discussion with researchers at Microsoft Azure for Operators (AFO) Research

Day 5: Presentation and discussion with researchers at Arm (Cambridge)

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)

As defined in https://europroofnet.github.io/objectives/, the STSM contributes to the following EuroProofNet objectives:

Research Coordination Objectives

3. Make techniques for program verification more effective and more accessible to all stakeholders.

Capacity Building Objectives

2. Act as a stakeholder platform in the field of formal proofs from its theoretical grounds to its industrial applications.

4. Ease access to formal verification techniques in education and other areas of science.

6. Transfer knowledge in terms of expertise, scientific tools and human resources across the different disciplines and between academia and industry.

8. 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 aim at building stronger industry collaboration in WG3 to work on impactful problems of practical interest.

We aim to contribute to the following deliverable:

- D11. Collection of verification challenges with summary of working recipes for verifying them.