Report on the outcomes of a Short-Term Scientific Mission[1]

Action number: CA20111

Grantee name: Muhammad Usama Sardar

Details of the STSM

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

Start and end date: 25-31 August, 2024

Description of the work carried out during the STSM

Description of the activities carried out during the STSM. Any deviations from the initial working plan shall also be described in this section.

(max. 500 words)

- I presented the research work on formal verification of attested TLS at Arm Cambridge which was attended by both systems architects, designers and formal verification teams of Arm (slides [1])
    - I had detailed discussions with Ionut Mihalcea, Simon Frost, Yogesh Deshpande and Shale Xiong from Arm about formal verification of attested TLS.
- I had discussion with host Dr. Lilia Georgieva Heriot-Watt University on our approach for formal analysis of attested TLS. We also discussed about the next deliverable, i.e., D11 Collection of verification challenges with summary of working recipes for verifying them.
- The visit to Microsoft Azure for Operators (AFO) Research could not happen at this time as the team in AFO is no longer in existence because of the change of priorities of Microsoft.
- Presentation and discussion at University of Stirling could not happen due to unavailability of staff during semester break. We are planning to have a virtual seminar instead. Instead of these two visits, I extended my stay at Heriot-Watt University.

[1] https://www.researchgate.net/publication/383658019_Presentation_Attested_TLS_for_Confidential_Computing

[1] This report is submitted by the grantee to the Action MC for approval and for claiming payment of the awarded grant. The Grant Awarding Coordinator coordinates the evaluation of this report on behalf of the Action MC and instructs the GH for payment of the Grant.

Funded by
the European Union

Description of the STSM main achievements and planned follow-up activities

Description and assessment of whether the STSM achieved its planned goals and expected outcomes, including specific contribution to Action objective and deliverables, or publications resulting from the STSM. Agreed plans for future follow-up collaborations shall also be described in this section.

(max. 500 words)

- We achieved the main goal of visit: I gave one hour seminar at Arm Cambridge. I established good connections, which I will follow-up for possible collaborations in order to achieve WG3 deliverables.

- The host Dr. Lilia Georgieva now has better understanding of our research and approach, and we will follow-up on this for possible collaboration in terms of how her work on using SPIN model checker, model analyzer Alloy, and AVISPA tool for security verification can possibly provide additional insights into attestation mechanisms for confidential computing.

- We have started work on the next deliverable, i.e., D11 Collection of verification challenges with summary of working recipes for verifying them. The challenges of practical importance to the industry include the following:

    - how to formally verify an underspecified protocol (i.e., attestation protocols in the context of confidential computing)?

    - how to deploy intra-handshake attestation protocol for the case when the load balancers cannot be modified?

    Until the next WG3 meeting, we will reflect the challenges in a report for deliverable D11.

- We are planning to have a follow-up (possibly virtual seminars) at the University of Stirling and the new Microsoft team and its partners.