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

Action number: CA20111

Grantee 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

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 gave a seminar at University of Edinburgh [1] (slides [2], video [3])
  - Follow-up discussion with Dr. Markulf Kohlweiss and his Ph.D. student Lorenzo Martinico at University of Edinburgh
- I gave a seminar at Heriot-Watt University [4] (slides [5])
  - Detailed discussion with host Dr. Lilia Georgieva on our approach for formal analysis
  - Follow-up discussion with Dr. Chengjia Wang at Heriot-Watt University for medical scenario use case
- We have written initial draft of 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).

[1] https://web.inf.ed.ac.uk/lfcs/events/lfcs-seminars/lfcs-seminars-2023/lfcs-seminar-tuesday-16-may-u-sardar

[2] https://www.researchgate.net/publication/370844935_Presentation_Comprehensive_Specification_and

[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.

_Formal_Analysis_of_Attestation_Mechanisms_in_Confidential_Computing

[3] https://www.youtube.com/watch?v=hqkXtGUpLUk

[4] https://ittgroup.org/seminars/

[5] https://www.researchgate.net/publication/370838319_Presentation_Comprehensive_Specification_and_Formal_Analysis_of_Attestation_Mechanisms_in_Confidential_Computing

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: 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 about their 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 written initial draft of 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), which we will keep improving.

- I gave one hour seminars at both University of Edinburgh and Heriot-Watt University. I established good connections at both universities, which I will follow-up for possible collaborations in order to achieve WG3 deliverables.