1st Workshop on

Industrial infrastructures Cyber Security for Advancing Collaborative manufacturing - ICSAC'2021

(Co-located with HiPEAC 2021)

January 18th, 2021 – Budapest, HU

**** Notice: HiPEAC and ICSAC will be held virtually for 2021, due to COVID restrictions ****

(check HiPEAC and ICSAC webpages periodically for any updates)

Call for papers

Industry 4.0 is based on the digitalization of processes and interconnection of equipment for improved operations, process optimization, and enhanced adaptability to marked needs. Looking beyond the single factory scope, collaborative manufacturing pushes the advantages of I-4.0 integration to the entire supply- and value-chain. The ICSAC workshop is focused around the cybersecurity challenges arising in collaborative manufacturing scenarios, to foster security solutions that can concretely improve trust and facilitate the transition to the I-4.0 paradigm. This workshop aims to be an open venue to discuss solutions able to (1) guarantee secure data exchange across the digital supply chain while providing high degree of resilience, reliability, accountability and trustworthiness, and (2) to address threat prevention, detection, mitigation, and real-time response. Some of the addressed topics (but not limited to them):

- Solutions for trusted computations at the edge, including trusted embedded platforms enablers (e.g. trusted execution environments based on commercial/open solutions, embedded cryptographic modules, root of trust solutions, secure boot, TPM),
- Solutions for confidentiality, including secure multi-party computations and homomorphic encryption,
- Solutions for trusted supply chain and secure transactions, including distributed ledger technologies and smart contracts,
- Solutions for secure communications and integration, including I-4.0 frameworks such us OPC-UA, UMATI, …
- Solutions for runtime network protection, including privacy-preserving embedded machine learning and novel approaches to anomaly detection,
- Solutions for managing Industrial IoT devices at scale, including PKIs and remote attestation,
- Pilots and success stories on security of collaborative manufacturing in the context of the I-4.0 vision.

This is the first edition of the ICSAC workshop, organized in the context of and with support from the EU H2020 project COLLABS 871518 (https://www.collabs-project.eu/). The workshop will host (a) two presentations from the COLLABS project, providing the vision and some technical achievements of the first year of the project, and (b) open presentation slots for papers selected among the submissions. Cybersecurity for industrial manufacturing infrastructures is a compelling and growing area for future embedded technologies, with an expected impact that will change radically the opportunities in the collaborative manufacturing domain. Cybersecurity is essential to provide adequate guarantees from the lowest to the highest layers of future manufacturing infrastructures.

Important Dates

- Submission Deadline: November 6, 2020
- Notification E-mails: December 11, 2020
- Camera-Ready Version: January 11, 2021

Quick Links

- Workshop site: https://www.collabs-project.eu/icsac-2021-workshop/
- Submissions: https://easychair.org/conferences/?conf=icsac2021
- HiPEAC 2021: https://www.hipeac.net/2021/budapest/#/

Guidelines for Submissions:

ICSAC'2021 will accept **full-paper (8-pages)** original and already-published scientific contributions (please indicate clearly, in the first page, previous publication venue, if any), as well as **short-paper (4-pages)** reporting on industrial experiences and pilots. Submissions to ICSAC'2021 shall be formatted according to EasyChair Proceedings format (https://easychair.org/publications/for_authors) and will be accepted only though the EasyChair page, reachable through the link from the ICSAC'2021 website and through the link in this call for papers. All submitted papers will be subject to blind review by program committee and external experts. The list of accepted papers will be made available before the workshop on the ICSAC website. Authors of accepted papers are required to ensure that at least one of them will be present at the workshop (either physically or virtually, depending on the COVID-related conditions, please check HiPEAC webpage for any updates). Authors will be notified of acceptance before the workshop (see Important Dates) and invited to submit a revised version of their contributions in the weeks after notification (see Important Dates). Selected papers, with original

contributions, will be invited to submit an extended version on a **special issue** of the **MDPI Applied Sciences journal** (IF 2.474), entitled "**Security management of 5G and IoT ecosystems**" (https://www.mdpi.com/journal/applsci/special_issues/5G_IoT_ecosystems).

Workshop Organization

Workshop Chairs (role: organization, paper selection)
Valerio Senni, RTX Research Center, Italy - e-mail: valerio.senni@rtx.com
Martin Wimmer, Siemens, Germany - e-mail: martin.r.wimmer@siemens.com

Program Committee (role: paper selection)
Fabio Federici, RTX, Italy - e-mail: fabio.federici@rtx.com
Srdjan Skrbic, Faculty of Sciences, University of Novi Sad - e-mail: msrdjan.skrbic@dmi.uns.ac.rs
Antonio Escobar, Infineon, Germany - e-mail: antonio.escobar@infineon.com

Web Chair (role: advertisement, support to submission)
Davide Martintoni, RTX, Italy - e-mail: davide.martintoni@rtx.com