Deliverable 5.2

Report on the dissemination, communication and exploitation activities in the second 12 months of Trusted IoT

Dissemination activities

Both in Germany and in Belgium, an **intermediate meeting** was held. In these meetings the research partners gave an update on the progress of the project to their national user groups. The Belgian meeting took place in Brussels, on **April 17th 2024**. The German meeting took place in Rostock, on **April 16th, 2024.**

The second broad dissemination event will take place on August 29, 2024 in Berlin, Germany. This event will be organised by GFaI.

On October 9th, 2024 an IMEC event will take place. The KU Leuven demonstrator will be shown during the presentation of the entire project. More info can be found here: https://www.wirelesscommunity.be/work-meetings/secure-over-the-air-firmware-updates-of-iot-devices/.

The Trusted IoT project was presented at “The 20th International Symposium on Applied Reconfigurable Computing - ARC 2024” in Aveiro, Portugal. The presentation was entitled “**Trusted Computing Architectures for IoT Devices**” and was given on March 21st, 2024. (link to symposium: https://www.arc2024.org/)

Communication activities

All the public communication on the activities within Trusted IoT appear on the website: https://jvliegen.github.io/trusted_iot_website/.

Trusted IoT is available on social media:

- Linked In: https://www.linkedin.com/company/trusted-iot/about/

One publication that was authored by KU Leuven was accepted at the “Malicious Software and Hardware in Internet of Things” conference. The title of the publication is “HAGAR: Hashgraph-based Aggregated Communication and Remote Attestation" and was presented in Italy on May 7th, 2024.

The research of the VUB were published in a journal paper, published on July 20 2024: Segers, L.; Talebi, B.; da Silva, B.; Touhafi, A.; Braeken, A. Trustworthy Environmental Monitoring Using Hardware-Assisted Security Mechanisms. *Sensors* **2024**, *24*, 4720. https://doi.org/10.3390/s24144720

The research results of TUD were published in the conference paper „Hardware-level Access Control and Scheduling of Shared Hardware Accelerators“ at the „27th Euromicro Conference Series on Digital System Design (DSD)“ that took place from 28-30.08.2024 in Paris. This paper won the best-paper-award.

Exploitation activities

At the **VUB**, the PIC32CM5164LS0064 has been used by student Borna Talebi for his master thesis. Borna further exploited the possibilities researched by Haythem (see D5.1) who did his thesis in 2022-2023. The results of the thesis were also published in the journal paper:
*Segers, L.; Talebi, B.; da Silva, B.; Touhafi, A.; Braeken, A. Trustworthy Environmental Monitoring Using Hardware-Assisted Security Mechanisms. Sensors **2024**, 24, 4720. https://doi.org/10.3390/s24144720.*
Borna investigated the impact of several security mechanisms such as TrustZone, data encryption and hashing. The first one allows to “hide” security mechanisms which allow the microcontroller to help generate new symmetric keys. The encryption and hashing are performed on data gathered from the attached sensors before they are transmitted to a remote computer. The biggest impact of TrustZone can be found on the memory allocation, where a substantial amount of the all types of memory (i.e. 20-50%) are allocated to TrustZone, leaving only 50-80% for the regular application. The encryption and hashing impact the application the most with regards to processing time, limiting the total transfer rates of up to 20-40kBps, depending on the selected encryption scheme.
Another master student, Veronika Shatz, uses the PIC32CK series microcontroller for advanced audio processing techniques with secure microcontrollers. Her defence is planned in January 2025.
Lectures about hardware security are also given by Prof. da Silva at the “S.he goes digital” program (Digital and IT Essentials). This long term program is provided to the applicants by the VUB and ULB.

The results of the VUB will be further utilised in 2 follow-up projects:

- Enact – Environmental effect on healthcare and wellbeing and active interventions
- Combine-IoT – Combining recent trends in Iot

The results of the project will be adapted and further optimised. The project will be converted into an open-source framework with several security features (such as published in our journal paper). This framework should, with minor modifications, be compatible with most of the ARM Cortex-M23 and ARM Cortex-M33 microcontrollers from the major vendors.

At the TUD, In the academic year 2023-2024 two Nano-Electronic System (NES) students finished their project works in the area of Trusted IoT:
Master student Saul Isaac Sanchez Flores developed an IP core for the scheduling of hardware tasks to hardware accelerators in temporal and spatial respect. The hardware tasks accelerate software tasks running under control of the microkernel based hypervisor L4Re. The hardware task scheduler includes an access control mechanism that prevents unauthorised access of software tasks to those hardware accelerators that the scheduler has not given access to. The hardware task scheduler could be deployed on a mobile robot in order to protect trusted hardware tasks from untrusted tasks.

The master student Xinyu Liu explored security threats mitigation using MicroROS and L4Re. The project included the port of ROS2/microROS to the ZynqMP platform with ARM

Trustzone support and to enhance the device’s cybersecurity to include hardware component peripherals.

The mobile robot platform developed at TUD is used for the lecture “Adaptive Systems for Robotics”, in which students are given an overview of the latest FPGA-based robotics accelerator designs and their optimization techniques. The lecture using the robot platform was held in the summer semesters 2023 and 2024.

At **KU Leuven** a proposal for a Bachelor thesis was proposed in the academic year 2023 - 2024. This topic was chosen and executed by a PXL student: Sem Kirkels. This student delivered very good work and he has gotten a summer job at ES&S, KU Leuven. During this student job, he contributed substantially to finish the demonstrator setup.
The calls for bachelor and master theses were also shared with the user committee.

With the results of the KU Leuven use-case, work was done to prepare for a follow-up, European funded project. At the moment of writing this deliverable, the European consortium is fixed. The academic partners are: KU Leuven (.be), VUB (.be), Chalmers (.se), Uni of Cagliari (.it) and Amsterdam University (.nl). From industry, there are Seafar (.be), Demcon (.nl), AnyWi (.nl), Beyond Vision (.pt), Abinsula (.it), Logiicdev (.at), and Nuromedia (.de). The Port of Antwerp-Bruges is also interested in the outcome of the project. This entire project proposal grew from the industrial use-case that was developed within this CORNET-funded project.