Deliverable 5.1

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

Dissemination activities

The first dissemination activity that was organized was the internal **kick-off meeting**. This meeting took place in a hybrid form in Brussels, on **September 15 2022**.

After a few months, two **kick off meetings** were organized for the national user groups. The German kickoff meeting took place on **December 1st 2022**. The Belgian kickoff meeting took place, a day later, on **December 2nd 2022**. Both these meetings were also organized in a hybrid form.

One-to-one meetings with members of the user group are:

- On **December 14, 2022**, the research partner **GFaI** engaged in a productive meeting with DSP Systeme GmbH. The primary agenda of this meeting was to deliberate on the project's scope and explore avenues for potential collaboration.
- Similarly, a significant meeting was held between **GFaI** and the Center for Connected Health Care UG on **June 29, 2023**. This meeting not only involved a comprehensive discussion on the project's current progress but also included valuable insights for charting the course of future tasks. In addition, the prospect of thematic overlaps was addressed, particularly concerning projects that have already reached completion.
- On **October 5, 2023**, **KU Leuven** researchers visited DroneMatrix. This meeting led to a short list of bare essentials that are required for a drone to fly. Also, the best fitting RISC-V implementations were discussed.

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 Diepenbeek, on **June 9th 2023**. The German meeting took place in Dresden, on **June 20th 2023**.

Finally, the first broad dissemination event took place on November 16th 2023 in Leuven, Belgium. Our presentations were part of the Industrial IoT Security Bill of Material (IIoTSBOM) event, organised by LSEC https://www.iiotsbom.com/up-and-coming-activities/iiotsbom-annual-update-16-11-23/).

Communication activities

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

During research for the use case of BTU, a method of hardening transition effect ring oscillator designs against process variations was discovered. The findings were published in the *ACM Transactions on Reconfigurable Technology and Systems (TRETS),* a well-known and reputable journal fitting the topic of the paper. It is titled “Increasing the Robustness of TERO-TRNGs Against Process Variation” and can be found under https://doi.org/10.1145/3597418. The findings are related to the use case of coarse-grained reconfigurable arrays (CGRA) in Industry 4.0, as discussed in deliverable D2.1, due to the ability of the discussed circuits to generate entropy in reconfigurable embedded systems. Entropy is needed to enable certain cryptographic functions that rely on randomness, e.g. generating new initialization vectors (IV) in AES-GCM, where the reuse of IVs degrade the security guarantees of the algorithm. Generating randomness in embedded systems is considered to be a difficult task, due to the limited and application-specific sources of entropy, indirectly affecting security functions.

Trusted IoT is available on social media:

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

During the research at the VUB 2 articles to a broader non-scientific audience have been published.

- The first one covers an article about how PUFs could better secure the IoT. The concept of PUFs are explained and categorized into different types of PUFs and their implementations on platforms. Some possible attacks are also being drawn. The article is published online and is accessible via: https://cybersecurity-bites.be/technologie/kunnen-physical-unclonable-functions-de-beveiliging-van-iot-verbeteren/
- The second article covers hardware modules that provide security features for embedded systems. A short description between hardware and software based security is shown. The Trusted Execution Environment (TEE) allows to separate the execution of the safe from the unsafe code to guarantee a secure isolation of code execution. Root of Trust (RoT) and Trusted Platform Module (TPM) are also highlighted as being part of the secure solution. The hardware must be able to support these features to obtain more safe embedded systems. The article is published online and is accessible via: https://cybersecurity-bites.be/technologie/hardwarebeveiliging-voor-ingebedde-systemen/

Exploitation activities

At the VUB, master student Haythem BOUGHARDAIN (academic year 2022-2023) investigated the currently offered security features by vendors for the low-end embedded platforms in his master thesis “Embedded Hardware Security: Impact of Security Features on Performance”. The different options include security modules like the “true random generation”, the TrustZone implemented in the Cortex-ARM23 and Cortex-ARM33 architectures, trusted platform modules (TPM) and hashing modules. He employed the PIC32CM5164LS0064 from Microchip, which implements the Cortex-ARM23 architecture and all the aforementioned security features. Haythem also performed a short comparison with the PIC32CM5164LE0064 microcontroller which does not offer the TrustZone features. He successfully defended his thesis in September 2023 with the conclusion that no impact difference is noted when utilizing the hashing and true random generator number modules are used on the 2 microcontrollers. However, when using the TrustZone function calls and execution time penalty between 1% and 3% has been noted compared to the same methods without TrustZone calls.
One student is currently working on the same topic during the academic year 2023-2024. This student will extend the work of the previous student and delve into more options with respect to the TrustZone and encryption mechanisms.

At the VUB, the PIC32CM5164LE0064 (without TrustZone) has also been used in the course “Geintegreerd Practicum Elektronica-ICT” (academic year 2022-2023) of the 3rd bachelor “Elektronica-ICT program” by the teaching assistant and the students. Students were asked to design and program a self-chosen application employing this microcontroller. The students also used the Microchip/MPLab environment to program this microcontroller. All but one group successfully managed to use and program this microcontroller and to complete this course during the academic year.
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.

At the TUD, one student work was finished in the academic year 2022-2023 in the area of low-power FPGA systems for mobile robots. Anastacia Grishchenko worked on a “Großer Beleg” with the topic “Synchronization Strategy for Hardware Tasks to Improve Energy Efficiency”. In this work, hardware tasks that are concurrently executed on hardware accelerators of an FPGA are synchronized so that Dynamic Voltage Scaling (DVS) can be applied in an enhanced way in order to improve energy efficiency.

Currently, two Nano-Electronic System (NES) students are doing project works in the area of Trusted IoT:
Master student Saul Isaac Sanchez Flores (academic year 2023-2024) is developing 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 unauthorized access of software tasks to those hardware accelerators that the scheduler has not given access to. The hardware task scheduler is planned to be deployed on a mobile robot in order to protect trusted hardware tasks from untrusted tasks.

The master student Xinyu Liu (academic year 2023-2024) explores security threats mitigation using MicroROS and L4Re. The project aims to port ROS2/microROS to the ZynqMP platform with ARM Trustzone support and to enhance the device's cybersecurity to include hardware component peripherals.

At KU Leuven both a proposal for a Bachelor thesis and a Master thesis were proposed in the academic year 2022 - 2023. Unfortunately, these topics were not selected by students. In the next academic year (23-24) both proposals will be put out again.
The calls for bachelor and master theses were also shared with the user committee. Through this user committee of Trusted IoT, 5 proposals have been added in the previous and the current academic year.

With the results of the KU Leuven use-case, work was done to prepare for follow-up research. In preparation of this follow-up project, discussions with industry took place. COMmeto and AnyWi (both members of the user committee) showed much interest. Outside the user committee we've also gained the interest of Signify, Thales, Airbus and Collins Aerospace.