Trusted IoT: meeting - minutes

Date:	Friday, June 9th 2023	
Location:	Technologiecentrum, Diepenbeek, Belgium	
Present:	*VUB:*	Laurent Segers, An Braeken
	KU Leuven:	Jo Vliegen, Md Masoom Rabbani, Nele Mentens
	Shayp:	Renaud Gonce
	COMmeto:	Ludo Cuypers, Jade Guo
	AnyWi:	Morten Larsen
	Verhaert:	Guus Colman (online)

These are the minutes of the first Belgian intermediate user group meeting. These will be published on the website: https://jvliegen.github.io/trusted_iot_website/

Re-introduction of Trusted IoT

A short presentation was given to guide this meeting. These slides can be found on the website.

Progress of VUB

A presentation was given by Lauren Segers to update the user group on the progress of VUB. These slides can be found on the website.

Progress of KU Leuven

A presentation was given by Jo Vliegen to update the user group on the progress of KU Leuven. These slides can be found on the website. A video was made to showcase the demonstrator. The link to this video can also be found on the website.

Demonstrators and discussions

These questions came up during the discussions at the demonstrators:

- Drones: safety is an important issue when flying over sensitive areas (schools, private terrain). It is advised to use multiple controllers for controlling the drone in case one controller fails.
- As readback of the configuration memory is possible, could this also be used to perform a secure update in the field ? This ties in with an earlier TeTra project: STRES.
- A few outstanding bugs in the readback were discussed
- Technical discussion about the power electronics of the ESC took place
- Firmware updates of energy harvesting devices were discussed.
- Microcontrollers: NXP offers high-end microcontrollers (I.MX family?) where operating systems can use TrustZone options.
- Texas Instruments offers a scala of microcontrollers but these do not tailor security features as such (TrustZone). These tailor performance.
- What do we understand as ultra-low poer microcontrollers? We see this as systems that go into deep sleep and only do some operations once every now and then (~30 minutes) and go into sleep again. One company (comment Morten Larsen) develops devices that run on the same battery for about 10 years. What about self-discharge of battery?
- Related to secure boot and ultra-low-power: how secure is the boot sequence of the microcontroller of an ultra-low-power MCU against possible attacks? It is known that secure booting on i.MX8 can be circumvented by UART tty or similar debugging ports.