OPEN-SOURCE RESILIENT HARDWARE AND SOFTWARE FOR INTERNET OF THINGS

HOW TO DESIGN EMBEDDED AND CONNECTED DEVICES TAKING ADVANTAGE OF OPEN SOURCE HARDWARE (AND SOFTWARE)

Issue 01

March 2023

horzion-orshin.eu

@ORSHIN_HE

orshin-horizon

Technical Lead

Daniele Antonioli

Eurecom

Scientific Lead

Benedikt Gierlichs

KU Leuven

Project Coordinator

Barbara Gaggl

Technikon Forschungs- und Planungsgesellschaft mbH

coordination@horizon-orshin.eu

Budget

€ 3.8 Million

100% EU-funded

Consortium

7 Partners

6 countries

Duration

36 Months

10/2022 - 09/2025

Message from the Coordinator

The intention of this newsletter is to open a new communication channel to provide news on the project progress and to discuss ongoing topics relevant to ORSHIN. This newsletter is intended for internal and external project partners, stakeholders and all other interested bodies. For more detailed information about the project, we invite you to visit our project website, which is constantly updated with the latest project related news: **horizon-orshin.eu.** The project has successfully started with a kick-off meeting in October 2022 in France. The event was hosted by Eurecom and coordinated by Technikon, with the main purpose of verifying plans and matching team members with first activities and to build the foundation for further collaboration. Hence, part of the agenda was the introduction of all the partners involved and their roles in the project. In addition, the work packages, including technical discussions and the planning of the next steps, took place. Since the kick-off, the consortium has been meeting virtually on a regular basis and face-to-face in January and is working relentlessly towards achieving the project objectives in this challenging and interesting topic.

Main Project Info

It is common wisdom that cyber security is only as strong as the weakest link in a chain. Therefore, the main challenge is to identify the critical points of IoT infrastructure. To address this issue, ORSHIN is creating the first generic and integrated methodology, called **trusted lifecycle**, to develop secure network devices based on open-source components while managing their entire lifecycle. This lifecycle defines how the safety objectives are translated into policies for defined phases. The ORSHIN project's main aim is to provide solutions to build reliable open-source hardware and linked devices. At the same time, this is intended to build a foundation for construction rely upon the safety properties of open-source components to advance their acceptance.

Project status after six months

In the first six months all work progressed according to plan. We have made technical progress in all areas related to the ORSHIN technical work packages.

Work Package 2 The team worked on the definition of a methodology for the development of secure open source hardware components (Trusted Life Cycle).

Work Package 3 The partners started developing hardware blocks with formal guarantees against relevant threats.

Work Package 4 Contributors worked on innovative testing methodologies to audit open-source hardware (OSH) components.

Work Package 5 The team assessed the security of pervasive constrained IoT devices and developed better security mechanisms usable with OSH.

There were no delays or roadblocks, all deliverables were submitted on time and we already published three research papers with ORSHIN results and we wrote three additional papers which are currently under review for publication.

Publications

In „**ProSpeCT: Provably Secure Speculation for the Constant-Time Policy**“ we present a generic formal processor model providing provably secure speculation for the constant-time policy and avoiding microarchitectural leaks for constant-time software (e.g., Spectre, LVI attacks). The paper also provides a prototype hardware implementation of ProSpeCT on a RISC-V processor and shows its low impact on hardware cost, performance, and required software changes.

In „**Low-Cost First-Order Secure Boolean Masking in Glitchy Hardware**“ we describe how to securely implement the logical AND of two bits in hardware in the presence of glitches without the need for fresh randomness. As a case study, we design, implement, and evaluate a DES core using our AND gate. The resulting DES engine shows no evidence of first-order leakage in a non-specific leakage assessment with 50M traces.

In „**Efficient attack-surface exploration for electromagnetic fault injection**“ we present a methodology to improve the effectiveness of electromagnetic fault injection physical attacks. In particular, we efficiently identify the subregion of the attack parameter space that maximizes the occurrence of an informative fault. The idea of this work consists of applying a multidimensional bisection method and exploiting the equilibrium between a pulse that is too strong and one that is too weak to disrupt the circuit‘s operation.

Past Events

Kickoff Meeting
20th - 21st October 2022
@Sophia Antipolis, France

Techincal Meeting
31st January - 01st February 2023
@Bergamo, Italy

Upcoming Events

ORSHIN workshop at RISC-V Summit Europe
09th June 2023
@Barcelona, Spain

All past and upcoming events can be found on the ORSHIN official webpage:

horizon-orshin.eu/events

We are excited to present our published research papers in the near future: We will present

- „**ProSpeCT: Provably Secure Speculation for the Constant-Time Policy**“ at USENIX Security 2023 in August.
- „**Low-Cost First-Order Secure Boolean Masking in Glitchy Hardware**“ at DATE 2023 in April.
- „**Efficient attack-surface exploration for electromagnetic fault injection**“ at COSADE 2023 in April.

Outlook

ORSHIN will be part of the 2023 RISC-V Summit Europe organized in Barcelona at the beginning of June. We will organize a workshop to discuss the project and its overarching goals with the RISC-V community.
Furthermore, there will be technical talks from members of the ORSHIN consortium covering research experiments at the intersection of ORSHIN and RISC-V. Finally, we will have an open session where participants can interact and foster new collaborations. We are excited about this workshop, as RISC-V is one of the hottest topics in the open-source hardware space, and with ORSHIN, we want to contribute to this cause.

The ORSHIN Consortium

The ORSHIN consortium consists of **seven partners** from six different countries (Austria, Belgium, Czech Republic, France, Germany, and Italy). It consists of a well-balanced mixture between academic and industrial players, from large semiconductor to small SMEs.
The present consortium of ORSHIN shows a various ability pool with the abilities and occurrence to tackle and resolve these challenges with explanation from Industry. Technikon has published videos on their website from **Daniele Antonioli**, **Benedikt Gierlichs** and **Maria Chiara Molteni** which will deliver an overview of ORSHIN aimed for the general public seeking more information.

TECHNIKON

Technikon Forschungs- und Planungsgesellschaft mbH
Austria [Villach]

KU LEUVEN

KATHOLIEKE UNIVERSITEIT LEUVEN
Belgium [Leuven]

EURECOM

EURECOM, FRANCE
[Sophia Antipolis]

NXP

NXP Semiconductors Germany GmbH
Germany [Hamburg]

SECURITY PATTERN

Security Pattern Srl
ITALY [Burago di Molgora]

Texplained
HARDWARE SECURITY INSIGHT

Texplained
FRANCE [Valbonne]

tropicsquare

Tropic Square s.r.o.
CZECH REPUBLIC [Prague]

The ORSHIN project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101070008.