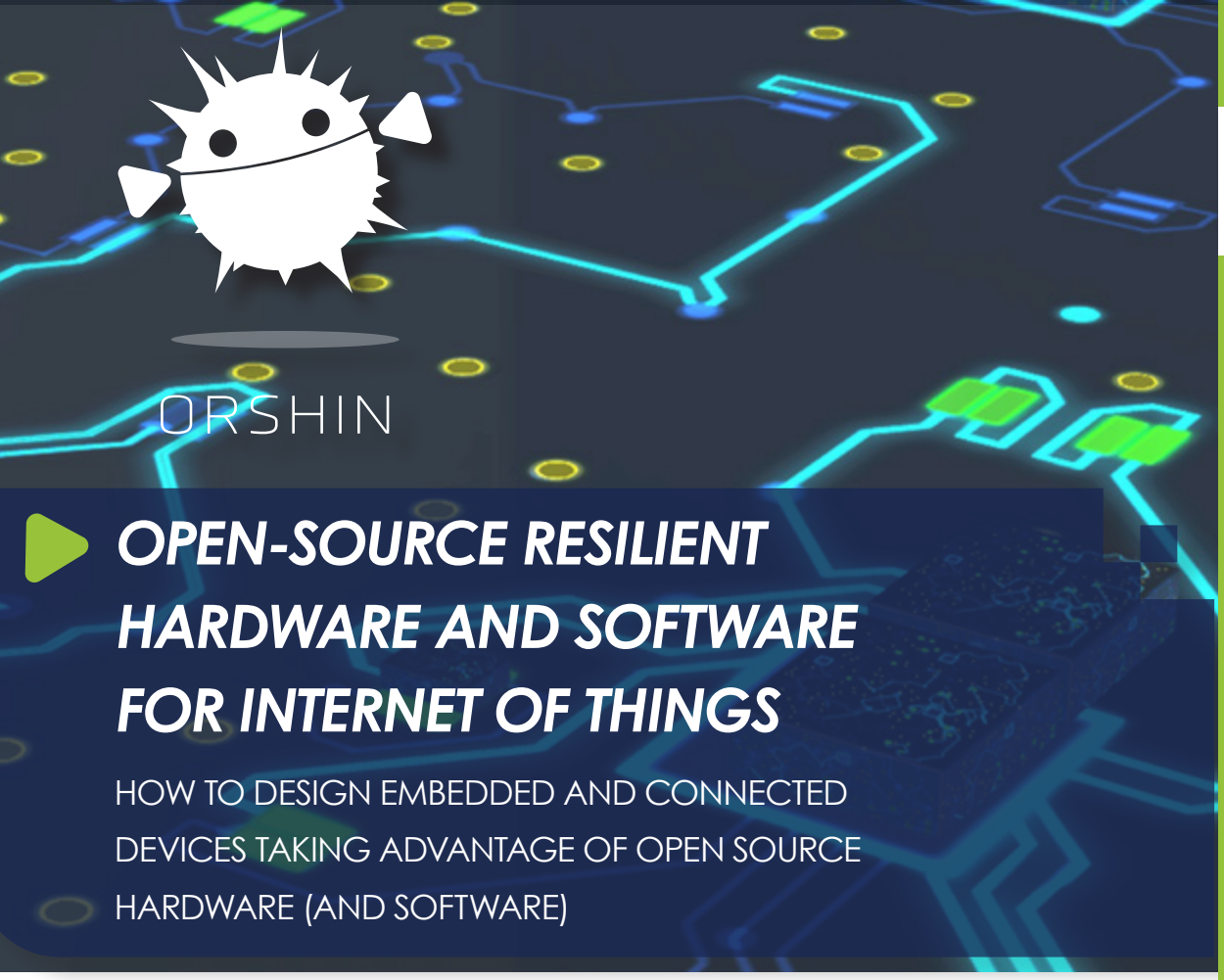

ORSHIN

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 04

Jan 2025

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

Project status, progress and results of the past months

The ORSHIN project is in the middle of the 2nd project period and achieving great results. During the past couple of months we worked on setting new standards related to security enhancement. We've been fostering transparency, trust and collaboration with the goal to build a future with smart and secure connected devices. The ultimate goal is to ensure that security is guaranteed throughout the lifecycle of open-source hardware devices. Therefore, we are currently developing new security models to enhance formal verification processes. We are creating practical and efficient hardware-augmented testing techniques for rigorous security audits. With this new approach, verifying the authenticity of a chip after manufacturing—ensuring it is free from backdoors or counterfeits hidden within the package—becomes significantly faster and more cost-effective. This enables systematic checks of IC integrity, safeguarding state sovereignty.

Another focus of the ongoing project work is to develop secure, privacy-preserving communication tools for both intra- and inter-device interactions. For example, we developed NSCP, a new secure channel protocol for intra-device communication. The protocol secures the embedded communication of critical components, like a microcontroller and a secure element in a smart card. It is based on the Xoodyak lightweight cryptographic primitive. Our evaluation shows that the protocol is up to four times faster than GlobalPlatform's Secure Channel Protocol 03 (SCP03), the de facto standard protocol for secure intra-device communication.

ORSHIN summer school

The ORSHIN project organizes a summer school, focusing on topics such as secure life cycle management of open source hardware, open source hardware with formally verifiable security guarantees, efficient firmware and hardware audits, secure and privacy preserving cryptographic protocols, Open Source Hardware supply chain verification, etc.

The summer school will take place from 7th – 10th September 2025 on the Greek island Crete and aims at bringing together Master/PhD students, academics and security experts from industry. For more information, please visit our website and don't miss your chance to register early: https://summer-school.info/

ORSHSEC workshop at CHES

On 4th September 2024 ORSHIN project partners organized the ORSHSEC workshop at CHES 2024 (Conference on Cryptographic Hardware and Embedded Systems) in Halifax, Canada. Organized by the International Association for Cryptologic Research (IACR), CHES is the premier event for research on the design and analysis of cryptographic hardware and software, bridging the gap between cryptographic research and practical engineering.
The ORSHSEC workshop focused on exploring the future of Secure Development Life Cycles (SDLCs) for open-source software and hardware. The event gathered brilliant minds to discuss essential topics such as the ORSHIN's Trusted Life Cycle for IoT devices and formal verification of security properties, both critical points for shaping secure and privacy-preserving technologies.
Our speakers from the ORSHIN project gave insightful presentations and their expertise is essential to driving progress in cryptographic security.

Publications:

- The paper **"AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling"** was published at ACM Transactions on Embedded Computing Systems.
- The paper **"Time Sharing – A Novel Approach to Low-Latency Masking"** was published at TCHES 2024.
- The paper **"Duplication-Based Fault Tolerance for RISC-V Embedded Software"** was published at the European Symposium on Research in Computer Security (ESORICS 2024).
- The paper **"Intellectual Property Exposure: Subverting and Securing Intellectual Property Encapsulation in**

Partners interviews

Video interview with Benedikt Gierlichs
Scientific lead giving insights into the last milestone achieved and outlook on the remaining project months.

Video interview with Guido Bertoni
CEO at Security Pattern sharing latest updates on the Trusted Life Cycle and innovative research on tiny tapeout chips.

Video interview with Stanislav Jerabek
Security researcher at Tropic Square talking about their role and perspective as an industrial partner in within ORSHIN.

Video interview with Clarisse Ginet
CEO at Texplained sharing insights about their critical role as a leader in hardware reverse engineering and security evaluation in the ORSHIN project.

Video interview with Aurélien Francillon
Professor at EURECOM shedding a light on the ORSHIN project, where open source hardware meets cutting-edge security.

Texas Instruments Microcontrollers" was published at USENIX Security Symposium 2024.

- The paper **"Libra: Architectural Support For Principled, Secure And Efficient Balanced Execution On High-End Processors"** was published at ACM CCS 2024.

(Complete list is on our website)

Conferences:

- **Real World Crypto 2025**, https://rwc.iacr.org/
- **Cascade**, https://cascade-conference.org/
- **CHES 2025**, https://ches.iacr.org/2025/
- **HARRIS Workshop**, https://harris2025.mpi-sp.org
- **Hardwear.io US**, https://hardwear.io/usa-2025/

Exchange with standardization bodies

To push toward standardization of our developed Trusted Life Cycle methodology, we continued discussions with European policy makers and standardization bodies during the past couple of months. We had interesting conversations with representatives from BSI, ENISA and ANSSI about how ORSHIN devices will be able to achieve similar or even better security ratings than current devices using security by obscurity. There will be further discussions and elaboration about the possibility to contribute to specific standardization initiatives to shape future certification of secure devices based on open-source hardware.

Trainings

Training sessions will be offered to industries, governments, and research institutions, with a focus on ensuring the security of open-source hardware throughout its lifecycle (design, manufacturing, deployment, etc.). Participants will learn to identify threats such as piracy, cloning, and counterfeiting, assess the hardware's resilience to these risks, and explore strategies to enhance its robustness against such threats.

Texplained will conduct training sessions quarterly, including hands-on workshops at their sample preparation laboratory, demonstrating the complete workflow needed for chip-level supply chain verification. Additional training sessions will be offered at conferences focused on reverse engineering and hardware security in the USA and Canada. For details about the trainings, visit Texplained's website. Registrations for conference-based trainings can be completed directly on the respective conference websites (hardwear.io and recon.cx).

Outlook

In the remaining project months we will focus on wrapping up the work in the technical work packages, on dissemination and making our results widely available, and in particular on finalizing the demonstrators for the various technologies and solutions we developed in the ORSHIN project. We will also work on planning our summer school and on preparing the technical contents.

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

Upcoming Events

Technical meeting
5th – 6th May 2025
Hamburg, Germany

Summer school
7th – 10th September 2025
Crete, Greece
https://summer-school.info/

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

horizon-orshin.eu/events