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 05
July 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 nearing the end of the 2nd project period, which marks also the overall end of the project, but it is still going full steam ahead: we continue to achieve great results!

The work in the technical work packages WP2 to WP5 was completed by end of June 2025. The remaining tasks are mainly centered around the establishment of the demonstrator platform, dissemination and project management.
We can proudly state that we achieved many very good research results which were published at top international venues!

ORSHIN progress

WP3: Work Package 3 focused on developing models for formal verification of hardware security, achieving several key results. Three hardware models were created to address micro-architectural side-channel leakage: ProSpeCT for speculative execution attacks, AMi for control flow leakage with code balancing and linearization, and Libra for secure balancing across more processors. Each model was also implemented in an open-source RISC-V processor.
For physical side-channels, WP3 emphasized the importance of balancing security and implementation cost, especially for IoT devices. A real silicon chip was designed, implemented, and manufactured to study gaps between theoretical and practical security, complemented by comparative experiments on FPGA platforms.
We also developed an open-source tool for analyzing hardware designs for side-channel leakage, using a fully open-source workflow. Several new countermeasures were developed: one challenges common assumptions in formal verification models to get security in practice at a lower cost, another is optimized for low-latency applications, and a third extends security to higher orders. All countermeasures were implemented, evaluated, and formally verified, demonstrating practical security and reduced implementation cost.
Overall, these results significantly improve the state-of-the-art in building side-channel resistant open-source hardware.

WP4: In Work Package 4 of the ORSHIN project, our team made major strides in improving the security of embedded and IoT systems—before they even hit the market.
We developed open-source tools that help detect vulnerabilities in firmware early on. These include a fault injection system that simulates hardware errors and a hybrid fuzzing tool that uncovers hidden software bugs faster and more effectively than traditional methods.
Our demonstrators show how combining hardware and software innovation can boost security:

- A fault injection platform for precise vulnerability detection
- A hybrid fuzzing system for deeper code analysis
- A firmware rehosting tool that allows safe testing in realistic conditions

All tools and platforms are open-source, encouraging collaboration and adoption across the tech community.
We also critically evaluated existing security standards and proposed new methods to better protect hardware against advanced attacks. Our approach shifts from "security by hiding" to "security by design," ensuring stronger protection from the ground up.
Extensive research has led to an innovative method for verifying the Open Source Integrated Circuits Supply Chain. This solution enhances manufacturer reliability and builds trust between manufacturers and chip makers during fabrication.

Together, these achievements pave the way for more secure, trustworthy embedded systems in the future.

WP5: In work Package 5 we focused on the development of innovative and practical methods to ensure security and privacy (S&P) for connected embedded devices, leveraging open-source hardware.
We addressed both intra-device and inter-device communications. We designed protocols to meet not only S&P requirements but also performance and usability constraints, ensuring they are suitable for real-world deployment.
The resulting protocols will mitigate security threats targeting ORSHIN devices and will deliver robust, practical, and novel mechanisms for secure communication and authentication.
In particular, we designed BlueBrothers, three new protocols providing essential and beyond essential S&P properties for inter-device communication. We implemented and tested them for Bluetooth Low Energy (BLE) and built a proof-of-concept demonstrator.
We also designed and developed the New Secure Communication Protocol (NSCP), which ensures both essential and advanced S&P properties for intra-device communication. The protocol was implemented and tested in a communication scenario between a Secure Element (emulated on an Artix-7 FPGA running a CORE-V processor core) and a master device (an STM32F4 board).
All the demonstrators will be evaluated, packaged and published in WP6 to maximise the ORSHIN project's impact and outcomes.

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/

📅 **Date:** 7th – 10th September 2025

📍 **Location:** Crete, Greece

🔗 **Details and registration:**
https://summer-school.info/

Final ORSHIN Project Workshop at CHES 2025 – Join Us in Kuala Lumpur

We're pleased to invite you to the **final workshop of the ORSHIN project** (Open-source ReSilient Hardware and software for Internet of thiNgs), held as an **affiliated event of CHES 2025** on its closing day in **Kuala Lumpur, Malaysia.**

📅 **Date:** Thursday, 18th September 2025

🕑 **Time:** Afternoon session 2pm - 5:30pm

📍 **Location:** CHES 2025 –
Affiliated Events, Kuala Lumpur

🔗 **Details and registration:**
ches.iacr.org/2025/affiliated.php#Event5

Over the past three years, ORSHIN has pushed the boundaries of transparent, reusable, and verifiable hardware security. This final workshop will highlight the project's achievements and offer a look ahead at the growing ecosystem of open silicon.

What to expect:

- Presentation of final results and public deliverables, including:
  - Pre-silicon security evaluation methodologies
  - Secure communication protocols for embedded systems
  - Mechanisms for enabling silicon-level supply chain auditability
- Live demos of project demonstrators, including the Secure Tetris Game and other real-world use cases
- Insights from industry adopters and contributors
- A panel discussion on the future of open and auditable security

Open to all CHES attendees, this workshop is a unique opportunity to engage with the ORSHIN community and help shape the path toward more trustworthy and transparent hardware systems.

Let's build the future of secure, auditable silicon – together.

Videos

ORSHIN Summer School
Informative video to disseminate the ORSHIN Summer School.

ORSHIN project update video
Project status and update video recorded at the meeting in Hamburg.

ORSHIN partner presentation - NXP
Meet the project partner NXP and their view on the potential of open source hardware.

Publications:

- The paper **Partial Key Overwrite Attacks in Microcontrollers: a Survey** was published at CASCADE 2025.
- The paper **Low-Cost First-Order Secure Boolean Masking in Glitchy Hardware** - full version was published in IEEE Transactions on Information Forensics and Security.
- The paper **Design, implementation and validation of NSCP: a New Secure Channel Protocol for hardened IoT** was published at DATE 2025.
- The paper **CheckOCPP: Automatic OCPP Packet Dissection and Compliance Check** was published at ACSW 2025.
- The paper **Wait a Cycle: Eroding Cryptographic Trust in Low-End TEEs via Timing Side Channels** was published at 2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).
- The paper **openIPE: An Extensible Memory Isolation Framework for Microcontrollers** was published at the 10th IEEE European Symposium on Security and Privacy (EuroS&P).

(Complete list is on our website)

Conferences:

- **USENIX WOOT 2025**, https://www.usenix.org/conference/woot25
- **VehicleSec 2025**, https://www.usenix.org/conference/vehiclesec25
- **CHES 2025**, https://ches.iacr.org/2025/
- **LightSEC 2025**, https://www.encrypt-on.com/activities/conferences/lightsec-2025/

Outlook

In the remaining months, one of the key tasks is the establishment of the demonstrator platform. This serves a user guide on how to reuse the delivery artefacts and reproduce the results for executable examples. Further, the project team is now preparing for our final two acts:

- the ORSHIN Summer School and
- the ORSHIN workshop at CHES.

We hope to meet you there!

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

Upcoming Events

Summer school
7th – 10th September 2025, Crete, Greece

ORSHIN workshop/final event at CHES
14th – 18th September 2025, Kuala Lumpur, Malaysia

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

horizon-orshin.eu/events