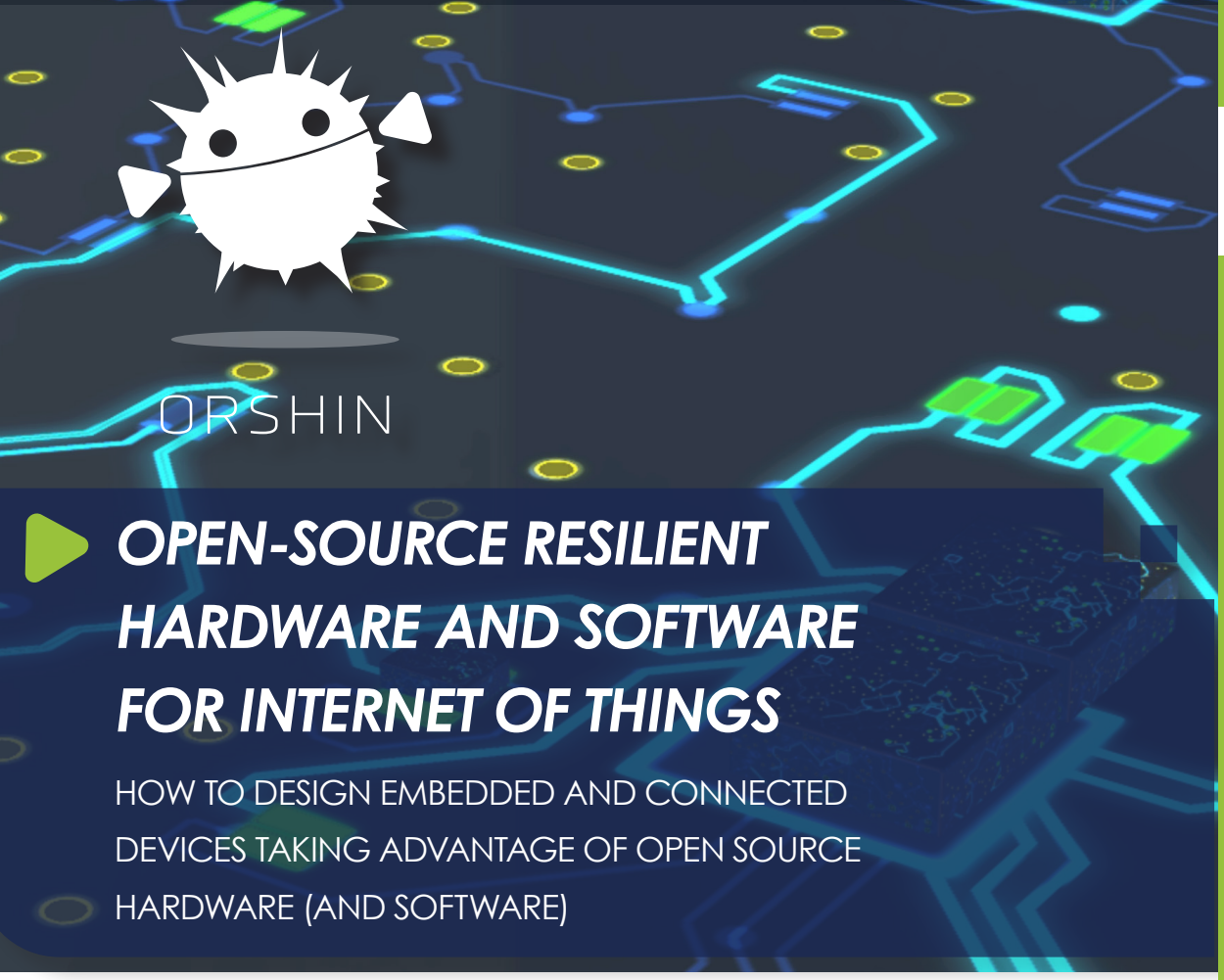

OPEN-SOURCE RESILIENT HARDWARE AND SOFTWARE FOR INTERNET OF THINGS

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

Issue 03
May 2024

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

Progress and results of the first period

During the first 18 months we laid the ORSHIN foundations. We developed a novel Trusted Life Cycle (TLC) that we use as the base to develop and manage an ORSHIN device. The TLC has six phases and is modeled after a chain that is as safe as its weakest link. The TLC embeds secure- and privacy-preserving by-design aspects, including early and incremental threat modeling and risk assessment.

Based on the TLC we developed new solutions in three key areas: hardware formal verification, low-level security testing, and constrained secure communications. We now provide an example of scientific contribution for each area (for more information, including a list of publications, please visit our website at https://horizon-orshin.eu/):

1. Hardware formal verification: in a paper titled **"ProSpeCT: Provably Secure Speculation for the Constant-Time Policy"** we propose a generic formal processor model providing provably secure speculation for the constant-time policy. For example, in some scenario we can guarantee no microarchitectural leaks from speculative or out of order execution. The paper was presented at the 2023 USENIX Security symposium together with an available, functional, and reproducible artifact.
2. Low-level security testing: in a paper titled **"Lightweight Countermeasures Against Original Linear Code Extraction (LCE) attacks on a RISC-V Core"** we study Linear Code Extraction attacks, which are a class of invasive hardware attacks capable of extracting a protected firmware. We develop three novel and effective hardware-level countermeasures to detect ongoing LCE by monitoring specific execution traces. We tested our lightweight solutions on a RISC-V core running on an FPGA. The paper was presented at the 2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) and won the best demo award.
3. Constrained secure communication: in a paper titled **"BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses"** we present the first evaluation of the

forward and future secrecy guarantees of Bluetooth. Bluetooth is daily used by billions of devices, including constrained ones, but it is unclear if a secure Bluetooth connection provides forward and future secrecy. These two essential properties protect past and future communication from key compromise attacks. In our work we discover protocol-level vulnerabilities and attacks capable of breaking forward and future secrecy of Bluetooth and we provide effective countermeasures embeddable in the Bluetooth standard or implementation-level mitigations. The paper was presented at the 2023 ACM Conference on Computer and Communications Security (CCS) and Chaos Communication Congress (37c3).

New publications:

- The paper **"Architectural Mimicry: Innovative Instructions to Efficiently Address Control-Flow Leakage in Data-Oblivious Programs"** was published at IEEE Symposium on Security & Privacy 2024. The authors are Hans Winderix, Márton Bognár, Job Noorman, Lesly-Ann Daniel and Frank Piessens.
- The paper **"An in-depth security evaluation of the Nintendo DSi gaming console"** was published at CARDIS 2023. The authors are Pcy Sluys, Lennert Wouters, Benedikt Gierlichs, Ingrid Verbauwhede.
- The paper **"Unveiling the Vulnerability of Oxide-Breakdown-Based PUF"** was published at IEEE Electron Device Letters. The authors are Pablo Saraza-Canflanca, Ferenc Fodor, Javier Diaz Fortuny, Benedikt Gierlichs, Robin Degraeve Ben Kaczer and Ingrid Verbauwhede.

(Complete list is on our website)

Potential impact of ORSHIN's results

ORSHIN's technical work packages provide research output and push the boundaries of the current scientific state of the art. This includes the creation of innovative research papers and prototypes, which are not just academic exercises, but generate significant academic impact and immediately stimulate future research.

Furthermore, the ORSHIN approach has great potential for adoption by industry as device manufacturers can leverage our TLC, tools, methodologies, etc. to build secure and trustworthy devices. The ORSHIN project provides formally verified, secure, open-source hardware blocks, reproducible and efficient security testing techniques, and secure and privacy-preserving communication protocols. We value the collaboration and contributions of all stakeholders in this process.

The TLC could become the industrial standard for developing dependable open-source hardware and software devices. Moreover, our framework for threat modelling could

Video material created

Explainer video
- Short video prepared by TEC
- Presenting the vision of the project
- Including main aims for next year

WP2 video
- SEC as WP2 led presented their work
- Focused on Trusted Life Cycle
- Put together by TEC to help inform the public regards the achievements of ORSHIN partners

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

Video interview with Jan Pleskac
CEO at Tropic Square emphasizing the significance of the project's focus on security, auditability, and the vital open-source aspect challenging industry norms

Video interview with Volodymyr Bezsmertnyi
PhD student at NXP focusing on presilicon firmware security

Newsletter Video
overview of what we have achieved so far

become a standard for assessing the risks of these devices. The ORSHIN project follows a holistic approach and besides the TLC further provides concrete advice for specific TLC phases, namely: design, implementation, evaluation and maintenance.

Exchange with standardization bodies

ORSHIN is also impacting the crucial and broad discussion around moving from closed-source to open-source hardware. We are pushing this important paradigm shift via constructive and frequent discussions with European policy makers and standardization bodies like ENISA, BSI and ANSSI. We discuss shortcomings of existing security certification methods with respect to open-source hardware as well as obstacles for the standardization of our TLC.

Conferences:

- IEEE Symposium on Security & Privacy 2024.
- 22nd Smart Card Research and Advanced Application Conference (CARDIS'23).
- ACM CCS Conference on Computer and Communications Security (CCS'23).

For further details, please visit the ORSHIN website.

Outlook

Having completed the first project period, we are excited about presenting our first results to the European Commission and external experts in the frame of the 1st review meeting. We have already plunged into the 2nd period having submitted further scientific papers at top venues, and there are more to come. We look forward to continuing discussions regarding standardization and certification with the relevant organizations.

Most importantly, we are excited about the **ORSHIN components' Secure Development Life Cycle (ORSHSEC) workshop**, which we organize as an affiliated event at CHES 2024 (4th – 7th September, Halifax/Canada). The workshop is focused on secure development life cycles for open-source software and hardware and will take place on 4th September 2024.

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

Upcoming Events

ORSHIN Review meeting
June 2024

ORSHSEC workshop at CHES 2024
4th September 2024
Halifax, Canada

CHES 2024
4th – 7th September 2024
Halifax, Canada

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

horizon-orshin.eu/events