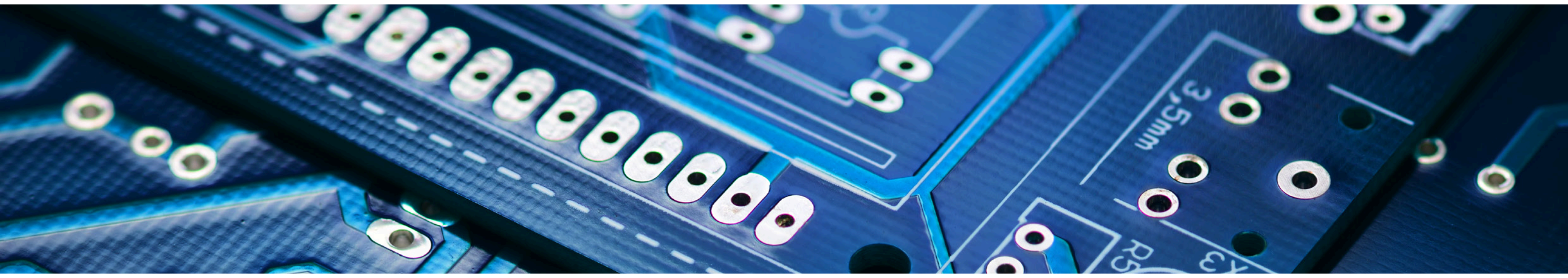
Open-source resilient hardware and software for Internet of Things

ORSHIN

The ORSHIN project aims to improve security for Internet connected devices through open-source hardware and software.

October 2022



Our society is evolving with increasing pace towards a digital society while we are embracing Internet connected devices, i.e., the Internet of Things (IoT), in urban and industrial environments. By connecting heterogeneous devices we trust their hardware and software manufacturers to provide secure and privacy-preserving services. The reliance of the (IoT) market on closed-source hardware and software solutions means often neither manufacturers nor customers get to know about security vulnerabilities of their devices.

The ORSHIN project embraces an open-source approach which reduces the risk of security threats staying undisclosed, as third-party experts are able to review security sensitive code in a collaborative and community environment. They uniquely look at the complete life cycle of an open-source IoT device, from design to its retirement, as a chain of trust to then design a generic and holistic methodology called the trusted life cycle.

The life cycle will specify how to translate abstract security goals (e.g., build a secure IoT product) into security policies for the different life cycle phases, and further into concrete security requirements for the building blocks of the product (e.g., use 128-bit keys). This includes the proposition of new models of security properties to extend formal verification to the secure, open-source hardware realm. Practical, fast, and hardware-augmented testing techniques will be developed to enable effective security audits, as well as methods for secure authentication and secure communication for connected devices in restricted environments. These interconnected developments and as such the holistic approach of the project will reduce security threats to open-source hardware for connected devices providing the next step in overcoming the challenge of weaknesses exposed by the IoT.

ORSHIN is a three-year European Union (EU) funded 3.8 million euro project starting in October 2022. Its overarching goal is reducing security and privacy risks associated with IoT devices through the opportunities of open-source hardware and software. The ORSHIN consortium includes renowned hardware and software cybersecurity experts from Security Pattern, Texplained and Tropic Square, three small medium enterprises (SMEs), KU Leuven and EURECOM university, and the NXP European semiconductor company. The consortium is coordinated by Technikon a private research service and engineering company based in Austria which manages multinational teams in the organization, execution, and assessment of research projects. Technikon is Europe‘s leading private company coordinating and disseminating technology-based cooperative European research projects.

For more information about the ORSHIN project, contact the coordinator directly:

Office:	TECHNIKON Forschungs- und Planungsgesellschaft mbH Burgplatz 3a, A-9500 Villach, AUSTRIA
E-MAIL:	coordination@horizon-orshin.eu
PHONE:	+43 4242 233-5571

Funded by the European Union

Funded by the European Union under grant agreement no. 101070008. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission-EU. Neither the European Union nor the granting authority can be held responsible for them.