Factsheet 01: Introduction to ORSHIN

In the world of security, the strength of a system is often determined by its weakest link. This challenge becomes even more daunting with open-source hardware, especially in the realms of the Internet of Things (IoT), industrial IoT, and critical infrastructure. These devices frequently operate in constrained environments with limited energy resources and often lack the necessary security and privacy guarantees.

How We Face These Challenges

Our primary goal is to establish a comprehensive methodology, known as the 'trusted life cycle,' for developing and managing connected devices based on open-source hardware. This lifecycle encompasses seven crucial phases: Threat modelling and risk assessment, Design, Implementation, Evaluation, Installation, Maintenance, and Retirement. By defining how to transform abstract security goals into specific policies and concrete requirements, we aim to fortify each phase of this lifecycle.

PROJECT AMBITION – REVOLUTIONIZING TRUST AND SECURITY

Increase Trustworthiness

The ORSHIN project is set to redefine how we perceive and ensure the trustworthiness of connected devices. By shifting from closed-source to open-source hardware, we open the doors for third-party inspections, drastically enhancing the reliability of these devices. No longer do we need to take the manufacturer's word for it—now, independent experts can verify the integrity and security of the hardware we rely on every day.

Transparecy and Audibility

In the spirit of openness, ORSHIN promotes the use of open-source hardware and software. This transparency allows us to establish trust without solely depending on the manufacturer. By making the inner workings of our devices visible to all, we can ensure they meet the highest standards of security and functionality.

IMPACT PATHWAYS – PIONEERING A NEW ERA OF OPEN-SOURCE

Paradigm Shift to Open-source

ORSHIN is a key initiative driving a new approach in the sector. By sharing knowledge across industries and researchers, we accelerate the time-to-market for innovative solutions. This collaborative approach not only speeds up development but also enhances the quality and security of the devices we create.

Enhanced Security Approaches

ORSHIN embraces the principles of Kerckhoffs, advocating for transparent and robust security implementations. By revealing the details of our security measures, we allow for broader scrutiny and confidence in their effectiveness, ensuring our devices are truly secure.

Key Outcomes

ORSHIN will focus on three key outcomes to mitigate security threats associated with open-source connected devices:

1. **Extending Formal Verification**
   Develop new models of security properties to enhance the verification processes for secure, open-source hardware.
2. **Effective Security Audits**
   Create practical, fast, and hardware-augmented testing techniques for rigorous security audits of open-source hardware and embedded software.
3. **Secure Communication Protocols**
   Develop secure and privacy-preserving protocols for both intra-device and inter-device communication, ensuring robust authentication and data protection.

Industry and Academic Collaboration

Our ambitious goals are supported by a powerful alliance: an international consortium of four high-tech SMEs, two academic partners, and a European semiconductor company. This collaboration combines cutting-edge industry expertise with academic rigor, driving forward innovations that will set new standards in open-source hardware security.

Join the Revolution

ORSHIN is setting a new standard in security enhancement. By fostering transparency, trust, and collaboration, we're building a future where connected devices are not just smart, but also secure. Join us on this journey to a safer, more trustworthy world of open-source hardware.

TECHNIKON · KU LEUVEN · NXP · Texplained HARDWARE SECURITY INSIGHT · EURECOM · SECURITY PATTERN · tropicsquare

Consortium
7 Partners
6 Countries

Budget
€ 3.8 Million
100% EU-funded

Duration
36 Months
10/2022 - 09/2025

Funded by the European Union

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