Open-source ReSilient Hardware and software for Internet of thiNgs

Follow ORSHIN on:

orshin-video-showcase

@ORSHIN_HE

ORSHIN-horizon-europe

Factsheet 02: Trusted Life Cycle

In the rapidly evolving world of technology, security is only as robust as the weakest link in a system. This principle is particularly challenging when applied to open-source hardware used on the Internet of Things (IoT), industrial IoT, and critical infrastructure. These devices often operate in constrained environments, with limited energy resources and frequently lack essential security and privacy guarantees.

The ORSHIN project is designed to address these challenges by creating a comprehensive and holistic methodology, known as the 'Trusted Life Cycle' (TLC). This lifecycle provides a structured approach to developing and managing connected devices based on open-source hardware, ensuring security at every stage.

Aims and Objectives

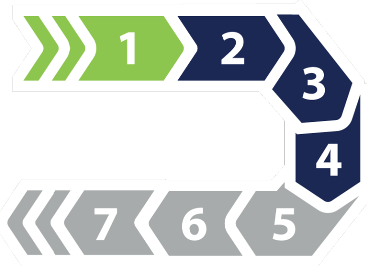
The primary aim of the ORSHIN project is to ensure that security is ingrained throughout the entire lifecycle of open-source hardware devices. It focuses on three key objectives: developing new security models to enhance formal verification processes, creating practical and efficient hardware-augmented testing techniques for rigorous security audits, and developing secure, privacy-preserving communication protocols for both intra-device and inter-device interactions.

These objectives are driven by an international consortium comprising four high-tech SMEs, two leading academic institutions, and a major European semiconductor company.

The Trusted Life Cycle (TLC): A Comprehensive Security Framework

The Trusted Life Cycle (TLC) is the cornerstone of the ORSHIN project, providing a detailed, methodical framework for the secure development and management of open-source hardware. The TLC is designed to address the unique challenges of open-source hardware by integrating security considerations into every phase of a device's lifecycle. This approach ensures that security is not an afterthought but a fundamental aspect of the entire development process.

Key Phases of the Trusted Life Cycle:



1. Threat Modeling and Risk Assessment
2. Design
3. Implementation
4. Evaluation
5. Installation Phase
6. Maintenance Phase
7. Retirement Phase

1. Threat Modeling and Risk Assessment

The Trusted Life Cycle begins with a security-by-design approach, where comprehensive threat modeling and risk assessment establish the essential security and privacy requirements. These requirements may come from external mandates, established standards, or specific cybersecurity analyses like threat enumeration. All requirements are validated through this process, forming the foundation for the entire lifecycle.

2. Design

In the Design phase, the hardware and all the relevant software components, are selected from open-source or defined to be implemented, if not available, based on the previously identified specifications and security requirements. This phase produces essential design artifacts such as schematics, system diagrams, and protocol sequences. The design approach focuses on minimizing security vulnerabilities, supporting secure implementation, and facilitating thorough testing and validation.

3. Implementation

During the Implementation phase, the design is translated into functional hardware and software/firmware components. This phase includes both in-house development and the integration of external or pre-developed third-party components. Open-source plays a key role in software development, though hardware development still largely relies on proprietary designs. This phase is critical for laying the groundwork for subsequent testing and validation.

4. Evaluation

The Evaluation phase involves rigorous testing of the complete device, and special attention for critical components. Various security testing are used to assess the system, including various fault injection methods. This phase provides crucial feedback to refine the design and implementation, ensuring high security and reliability before deployment.

5. Installation Phase

In the Installation phase, embedded devices are deployed, often in challenging environments. It is essential that the installation adheres strictly to the intended security context and threat modeling to maintain security integrity.

6. Maintenance Phase

The Maintenance phase spans the entire operational life of the product, from installation to retirement. During this phase, devices are remotely monitored, maintained, and updated, with continuous performance checks. Ongoing security monitoring is critical to address any vulnerabilities that may arise post-release, ensuring the product remains secure and functional.

7. Retirement Phase

The Retirement phase marks the end of the device's lifecycle. This phase focuses on securely erasing all sensitive data and revoking any access privileges to prevent data breaches or unauthorized access after the device is decommissioned. By following these procedures, the device can be securely retired, protecting sensitive information.

Impact and Innovation

The ORSHIN project represents a significant advancement in the security of open-source hardware. By embedding security into every phase of the lifecycle, ORSHIN not only enhances the trustworthiness of connected devices but also sets new standards for secure hardware development. The Trusted Life Cycle ensures that security is a continuous process, from the initial design to the final retirement of the device.

Key Innovations:

- Holistic Security Integration: The TLC ensures that security is not a separate, isolated concern but an integral part of every stage in the hardware development process.
- Enhanced Open-source Trust: By leveraging the transparency and collaborative nature of open-source components, the TLC facilitates a more secure and trustworthy development process.
- Future-proofing IoT Security: The TLC's comprehensive approach addresses both current and emerging security challenges, making it a vital tool for the future of secure IoT and industrial IoT development.

Conclusion

The ORSHIN project is pioneering a new era in secure hardware development through its Trusted Life Cycle methodology. By fostering a culture of security from the ground up, ORSHIN is revolutionizing the way we approach the development of open-source hardware for IoT and industrial applications. The TLC's structured, security-focused approach ensures that devices are not only functional but also resilient against the ever-evolving landscape of cyber threats.

Join us in this groundbreaking journey to create a safer, more secure world of connected devices.

TECHNIKON · KU LEUVEN · NXP · Texplained HARDWARE SECURITY INSIGHT · EURECOM Sophia Antipolis · 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.