Factsheet 04: Community-Driven Security Improvements in Open Source Components

Ensuring the security of open source components has been increasingly important as open source becomes more involved with connected devices and security systems. ORSHIN aims to strengthen the security processes behind open-source hardware and software by developing methodologies that provide structure, design formal verification and auditing processes, and defining clear best practices.

A key feature of open source is in its ability for community contributions. By combining community-driven innovation with rigorous, standardized security processes, ORSHIN helps build a more resilient and transparent ecosystem – aligning with emerging regulations like the EU Cyber Resilience Act.

ORSHIN's objective is to ensure that open-source components are not only collaborative and innovative but also trustworthy and secure for use in critical IoT infrastructure.

The Role of Community in Open Source

The open source community comprises a diverse network of contributors, each bringing unique expertise and perspective to security enhancement:

- Security researchers identify potential vulnerabilities
- Developers implement reviewed solutions
- User provides real-world testing and feedback

This collaborative environment enables ongoing comprehensive code reviews and security testing that closed systems don't offer due to its need of administrative barriers and permission-based procedures.

The shared knowledge base facilitates information distribution and exchange to support transparency to ensure trust in the security implementation.

The Benefits of Community-Driven Security in Open Source

- **Vulnerability Detection:** The continuous review process increases the detection speed of security issues. Public disclosure creates accountability and incentive to promptly address vulnerabilities.
- **Enhanced Transparency:** Open source provides complete visibility into security implementations for thorough verification of security measures. The open review process helps prevent the introduction of backdoors or hidden vulnerabilities.
- **Collaborative Innovation:** The community model encourages the discussion and sharing of best practices in security innovations. Security standards are tried and tested by a mass amount of users.

Best Practice and Guidance for Community-driven Improvement

Security Development Lifecycle

Secure development practice must be built in the process from the beginning. Regular security audits help identify potential vulnerabilities and areas of improvement. All security measures and controls need clear documentation, allowing new contributors to understand and follow established protocols.

ORSHIN has developed the Trusted Life Cycle (TLC) to provide structure and milestones to aim towards in the secure development process.

Community Management

Have clear procedures for handling security-related contributions and reports. Contributions and reports from community contributors should undergo stringent security review before acceptance.

Having a clear process for responsible disclosure streamlines the process towards implementing a resolution for discovered issues.

Transparent Communication

Up-to-date security documentation helps all community members understand the current security practices and requirements. Accessible information about vulnerability resolution helps prevent similar issues not only for the same project but for across other projects. Having open channels specifically for security discussions allow community members to raise concerns and share insights.

Real World Case Studies and Examples

- Linux - open source software
- Tropic Square - TROPIC01 auditable secure chip
- OpenHWGroup - RISC-V cores

Conclusion

The role of community collaboration and independent validation is vital in advancing secure hardware development practice. Community-driven security improvement in open source projects demonstrates the power of collaborative security enhancement.

By following established best practices and methodologies that ORSHIN aims to provide as well as leveraging community expertise, businesses and projects alike can build more secure and resilient systems from design to implementation to maintenance throughout the whole device lifecycle.

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.