REWIRE

REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems

Newsletter Issue 10|Webinars Edition

Welcome to the 10th REWIRE Newsletter,

REWIRE is a 3-year Research and Innovation Action, started during October 2022, and funded under Horizon Europe.

REWIRE envisions a **holistic framework for continuous security assessment** and management of open-source and open-specification hardware and software for IoT devices, throughout their **entire lifecycle**, under the **zero-trust** concept, adhering to the **security-by-design** principle and providing **cybersecurity certification**.

In this issue

Our newsletter is published periodically offering updates on project achievements and results.
Subscribe here to receive REWIRE newsletter at your inbox.

Funded by the European Union

REWIRE Cybersecurity Awareness Webinar Series

Trust or Bust: Reinforcing the IoT Interoperable Security Stack with Efficient Secure Lifecycle Management Capabilities – The RISC-V Opportunity

Date: 09/05, 12/05/, 19/05 2025
Location: Online
Host: ENTRUST and **REWIRE** Horizon Europe projects

The REWIRE Cybersecurity Awareness Webinar Series, co-organized by the EU-funded research projects REWIRE and ENTRUST, was a resounding success. We delved into the critical challenges of security, trust, and privacy within complex IoT "Systems-of-Systems" and explored groundbreaking solutions designed to build a secure foundation for the future.

For those who couldn't join us live or wish to revisit the deep technical discussions, we are pleased to announce that recordings of all three sessions are now available on YouTube. These sessions featured experts from academia and industry showcasing real-world applications and demonstrating the innovative solutions developed within these pioneering projects.

About the Projects

ENTRUST aims to ensure end-to-end trust management of medical devices strengthening trust & privacy in the entire medical ecosystem. The breakthrough solutions that ENTRUST provides, will not limit the applicability of connected medical devices, by enclosing to them cybersecurity features including formally verified trust models, risk assessment process, secure lifecycle procedures, security policies, technical recommendations and the first-ever real-time Conformity Certificates to safeguard connected medical devices.
More info: https://www.entrust-he.eu/

REWIRE, an EU-funded project, introduces a holistic cybersecurity platform designed to continuously monitor open-source and open-specification hardware and software for IoT devices, assessing potential threats and addressing cyber risks such as viruses, data breaches, and denial-of-service attacks in today's increasingly digitalised and connected world. The platform will provide protection throughout the IoT device lifetime. REWIRE will also introduce a cybersecurity certification procedure that is in line with the new EU cybersecurity regulations. The novel solutions will be tested across three pilot environments – automotive, smart cities and smart satellites – paving the way for more secure data exchange.
More info: https://www.rewire-he.eu/

09/05 Highlights

Webinar 1: Reinforcing Trust Assessment Mechanisms through AI-based Misbehavior Detection

This insightful session focused on the challenge of detecting sophisticated runtime threats in vast IoT networks. Our speakers explored how artificial intelligence can be harnessed as a dynamic layer to significantly enhance the accuracy of trust assessment frameworks.

Funded by the European Union

REWIRE Cybersecurity Awareness Webinar Series

Webinar 1: Reinforcing Trust Assessment Mechanisms through AI-based Misbehavior Detection

The webinar kicked off with a visionary keynote from UBITECH on the REWIRE project's approach to trustworthy systems. This was followed by a deep dive from Suite5 into the practical implementation of AI-driven misbehavior detection mechanisms, demonstrating how machine learning models can identify subtle anomalies and flag deviations that signal compromise. The session concluded with a lively Q&A, addressing questions on model training and integration.

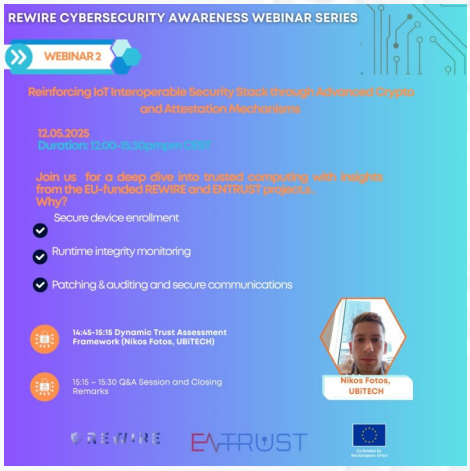
[CLICK HERE TO WATCH WEBINAR 1]

12/05 Highlights

Webinar 2: Reinforcing IoT Interoperable Security Stack through Advanced Crypto and Attestation

This packed, extended session **provided** a comprehensive deep dive into the core technologies that create a secure and interoperable security stack. The event **featured** seven presentations that covered the entire device lifecycle, from a unifying vision for a harmonized Trusted Computing Base to specific technical breakthroughs. Attendees **learned** about securing software updates with advanced encryption, implementing secure updates on RISC-V, and innovative protocols for zero-touch onboarding. Experts from the University of Murcia **detailed** enhanced privacy for conformity certificates, while the UBITECH team **showcased** their groundbreaking work on developing efficient and scalable remote attestation mechanisms specifically for RISC-V devices. The webinar **successfully synthesized** these technologies into a coherent framework for dynamic trust.

[CLICK HERE TO WATCH WEBINAR 2]



Funded by the European Union

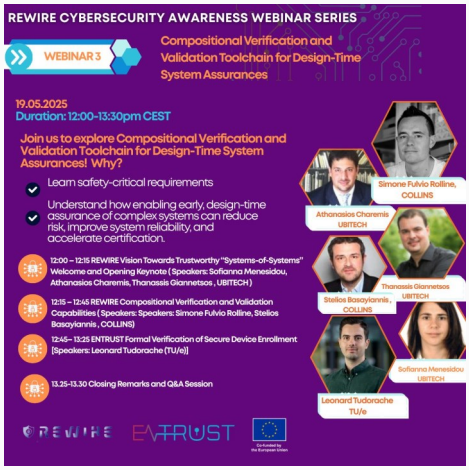
REWIRE Cybersecurity Awareness Webinar Series

19/05 Highlights

Webinar 3: "Compositional Verification and Validation Toolchain for Design-Time System Assurances"

Our final webinar **highlighted** the paramount importance of preventing vulnerabilities at the design phase. The session **focused** on how formal methods and compositional verification tools are used to ensure design-time correctness of hardware configurations for RISC-V devices. Experts from COLLINS **presented** REWIRE's capabilities, explaining how they ensure hardware configurations are correct-by-construction. This was **followed** by a presentation from Eindhoven University of Technology, which **showcased** ENTRUST's work on the formal verification of secure device enrollment procedures—a critical process for medical devices and other high-stakes applications. The webinar **effectively demonstrated** how these techniques provide the highest level of assurance and create a verified foundation for runtime security.

[CLICK HERE TO WATCH WEBINAR 3]



Press Release

EU-Funded Initiatives Unite to Address Critical Cybersecurity Challenges in the Internet of Things

The REWIRE Cybersecurity Awareness Webinar Series, a collaborative effort between two major EU-funded research projects, successfully concluded this week. The series, titled "Trust or Bust," brought together leading experts to tackle the pressing security challenges posed by the rapidly expanding Internet of Things (IoT).As billions of new devices connect to global networks—from smart cities and medical equipment to autonomous vehicles—ensuring their security and maintaining user trust has become a paramount concern. The "Trust or Bust" series addressed critical security challenges in the expanding Internet of Things (IoT) landscape. Sessions focused on AI-powered threat detection, hardware-level security, and verifying device trustworthiness throughout its lifecycle.The series demonstrated how these security innovations are being applied across critical sectors including healthcare, automotive and public infrastructure.

For more information:

REWIRE:https://www.rewire-he.eu/

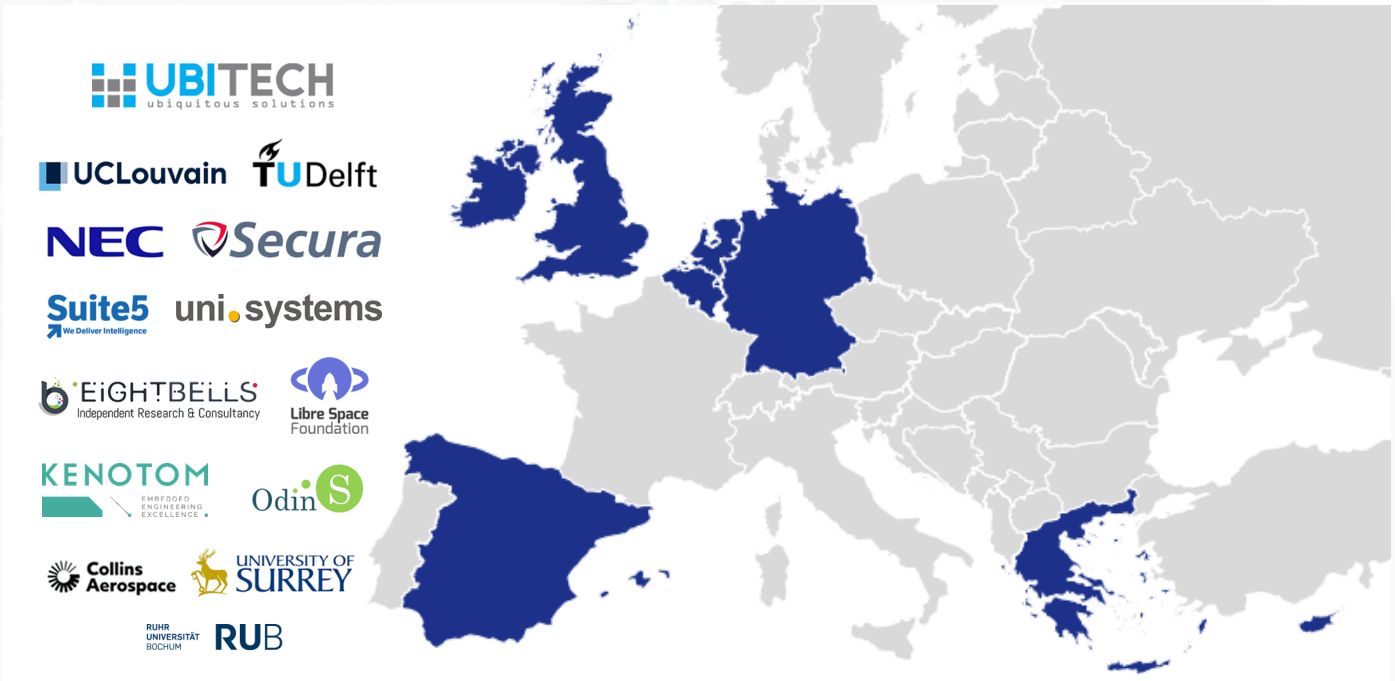
ENTRUST: https://www.entrust-he.eu/

Funded by the European Union

At a glance

Rewire consortium

REWIRE brings together 14 partners form 8 European countries, providing all the required expertise for achieving the project's ambitious objectives.



Fact Sheet

Title	Rewiring the Compositional Security Verification and Assurance of Systems of Systems Lifecycle
Acronym	REWIRE
GA No	101070627
Start	01 October 2022
End	30 September 2025
Budget	4.158.961 €
EU Fund	4.158.961 €
Topic	HORIZON-CL3-2021-CS-01-02
Scheme	RIA - Research and Innovation action

rewire-he.eu rewire-horizoneu-project @RewireProject @REWIRE-HE-project

REWIRE newsletter is published every three months, offering the latest news and advances of the project!
Subscribe here to receive REWIRE newsletter at your inbox.

Funded by the European Union