REWIRE

REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems

Newsletter Issue 3 | July 2023

Welcome to the 3rd 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 every 3 months, offering updates on project achievements and results.
Subscribe here to receive REWIRE newsletter at your inbox.

Funded by the European Union

REWIRE Research Pillars

Design of Flexible Hardware Architectures Converging Security and Performance

This research pillar focuses on Model-Based Engineering (MBE) and the Zero Trust concept in the realm of cybersecurity. Architecture Analysis and Design Language (AADL) is at the core, enabling the design of complex real-time embedded systems by modeling software and hardware components. AGREE and Resolute are crucial tools that support formal analyses and assurance arguments within AADL models. The preference for AADL over SysML is due to its hierarchical architecture, rigorous runtime semantics, and extensibility for evolving Cyber-Physical Systems (CPS) design. This research pillar aims to explore deductive verification with Coq and model checking for formal requirement verification. Model checking has become an industry standard for digital systems verification, particularly in hardware security and RISC-V designs.

Formal Verification and Validation of Secure and Trusted Operation of Crypto Mechanisms.

This pillar focuses on formally verifying and validating cryptographic mechanisms for secure and trusted operations. Authenticated Encryption (AE) schemes, combining integrity and confidentiality, offer strong security and performance. It addresses security concerns of cryptographic protocols during implementation, with a focus on physical security against side-channel attacks. Lightweight cryptography targets resource-constrained devices, providing solutions that balance security and performance. Leakage-resilient cryptography introduces countermeasures against side-channel information leakage. Formal verification techniques are utilized to ensure the security of AE schemes, allowing for high-level descriptions to be checked against machine-generated code. This pillar aims to enhance cryptographic mechanisms' reliability and trustworthiness.

Trust Governance of IoT Environments and Embedded Devices Using Open Standards.

This pillar presents a Trusted Execution Environment (TEE) using open standards for IoT environments and embedded devices. The proposed TEE is based on RISC-V architecture, offering customizable security features and compatibility across various platforms. Intel Software Guard Extension (SGX) is a hardware-based isolation extension used for trusted applications, but it has vulnerabilities to side-channel attacks. RISC-V's modular design allows for easy extension with different security primitives, such as Physical Memory Protection (PMP) registers and Input/Output Memory Management Unit (IOMMU), ensuring isolation and control over memory access for TEEs. Keystone, an open-source TEE framework, is chosen for REWIRE, offering programmability, agile patching, and verifiability as advantages over proprietary solutions.

Runtime Monitoring of IoT Trustworthiness and Operational Assurance of SoS.

This research pillar ensures the trustworthiness and operational assurance of IoT systems through runtime monitoring. It explores "Roots of Trust" for establishing secure foundations and investigates "Remote Attestation" schemes, particularly emphasizing control flow attestation and its challenges. The research delves into runtime tracing technologies to enable effective control flow attestation, addressing solutions and challenges in IoT and embedded systems.

Funded by the European Union

REWIRE Research Pillars

Decentralized identity management & trust-aware continuous authentication & authorization

This research pillar explores the advancements in Self-Sovereign Identity (SSI) through decentralized identity management using technologies like Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). SSI provides individuals with control over their digital identity without relying on centralized authorities. DIDs serve as unique identifiers and are standardized by the World Wide Web Consortium (W3C). VCs enable holders to prove their credentials and create verifiable presentations (VPs) for authorization. The research evaluates the use of distributed ledgers, like Blockchain, for trust establishment in SSI and addresses challenges related to identity revocation and renewal. The technologies are already being used in real-world applications, such as the European Blockchain Partnership (EBP) and Microsoft Azure Active Directory Verified Credentials. The research also explores how VPs can be utilized for authorization, taking into account device trustworthiness and privacy considerations.

Firmware and Software Automated Validation and Vulnerability Analysis

This research pillar focuses on automated validation and vulnerability analysis of firmware and software in the REWIRE project. It employs static and dynamic analysis techniques, supporting firmware images in various formats and utilizing bytecode analysis for unpacked firmware. Tools like Binwalk and BANG are used for accurate unpacking. The analysis can be performed statically, dynamically, or emulating the entire firmware. Multiple static and dynamic techniques are employed, including taint analysis, control flow graph analysis, dynamic taint analysis, and concolic execution. Binary instrumentation is used for fuzzing and concolic execution, and the combination of both techniques is applied for analysis. The research emphasizes the importance of runtime monitoring, particularly for control flow integrity in embedded devices, and addresses vulnerabilities like control flow hijacking in the RISC-V architecture.

Service Certification & Auditing through Blockchain-Based Secure Info & Data Exchange

This research pillar leverages blockchain technology for secure and decentralized service certification and auditing. Blockchain offers a transparent, immutable, and verifiable platform for service providers to securely store and exchange data. Researchers are exploring the use of trusted hardware like Intel SGX or ARM TrustZone in combination with decentralized oracles to create secure and efficient protocols. The pillar also explores the balance between on-chain and off-chain data management, considering factors like transparency, cost-effectiveness, and network performance. Smart contracts automate data collection processes, while blockchain wallets and verifiable credentials provide secure key management and identity verification. Access control mechanisms are crucial for maintaining network security. Blockchain technology presents a potential solution for data auditing and certification, replacing centralized services with a more secure and cost-effective approach.

Secure Distributed Service Operation through Misbehavior Detection

This research ensures the secure operation of distributed service environments like IoT and cloud computing, providing critical services with confidence. These environments consist of multiple heterogeneous devices communicating, but security and privacy challenges arise due to increasing sophistication of attacks. Misbehavior detection systems are needed to detect malicious actors pretending to be network nodes. Machine learning is applied in these systems, with AI-based detection becoming essential due to limited resources on IoT devices. Traditional learning and deep learning approaches, as well as advanced concepts like federated learning, reinforcement learning, and generative adversarial networks, offer promise in detecting misbehavior. AI-based misbehavior detection offers insights into network behavior and potential security issues.

Funded by the European Union

Publications, Events & Media

Scientific publications

We present below the list of papers submitted and accepted during the period April-June 2023 that carry acknowledgement of REWIRE project. For the complete list of research papers, please visit https://www.rewire-he.eu/publications/.

◊ Malaquias, F.L., Asavoae, M., Brandner, F. (2023). *From the Standards to Silicon: Formally Proved Memory Controllers*. In: Rozier, K.Y., Chaudhuri, S. (eds) NASA Formal Methods. NFM 2023. Lecture Notes in Computer Science, vol 13903. Springer, Cham.

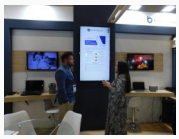
Events

REWIRE @ DATE2023

Our colleagues from UCLouvain participated in DATE 2023 Conference, entitled "Design, Automation and Test in Europe Conference". Read more at https://www.rewire-he.eu/rewire-date2023/.

REWIRE @ DEFEA2023

REWIRE has been presented at the exhibition booth of project partner Eight Bells, during the Defence Exhibition Athens (DEFEA) 2023. Read more at https://www.rewire-he.eu/rewire-defea2023/.

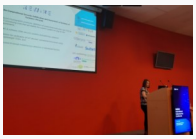


1st Plenary Meeting

REWIRE consortium partners gathered in Louvain-La-Neuve, Belgium, on 6 and 7 June 2023, for the 1st Plenary meeting, that was kindly hosted by project partner UCLouvain, in hybrid form. Read more at https://www.rewire-he.eu/1st-plenary-meeting/.

PUZZLE ICC

REWIRE was presented at PUZZLE International Cybersecurity Conference, which took place at Novi Sad, Serbia, during June 21st 2023. Read more at https://www.rewire-he.eu/puzzle-icc/



REWIRE poster presented at ECCWS2023

Our colleagues from project partner Eight Bells participated in ECCWS2023, which took place in Athens, on June 22-23, 2023, hosted by the Hellenic Airforce Academy. Read more at https://www.rewire-he.eu/rewire-poster-presented-at-eccws2023/.

#REWIREBlog

Here is the list of posts for period April-June 2023. Stay tuned at https://www.rewire-he.eu/blog/.

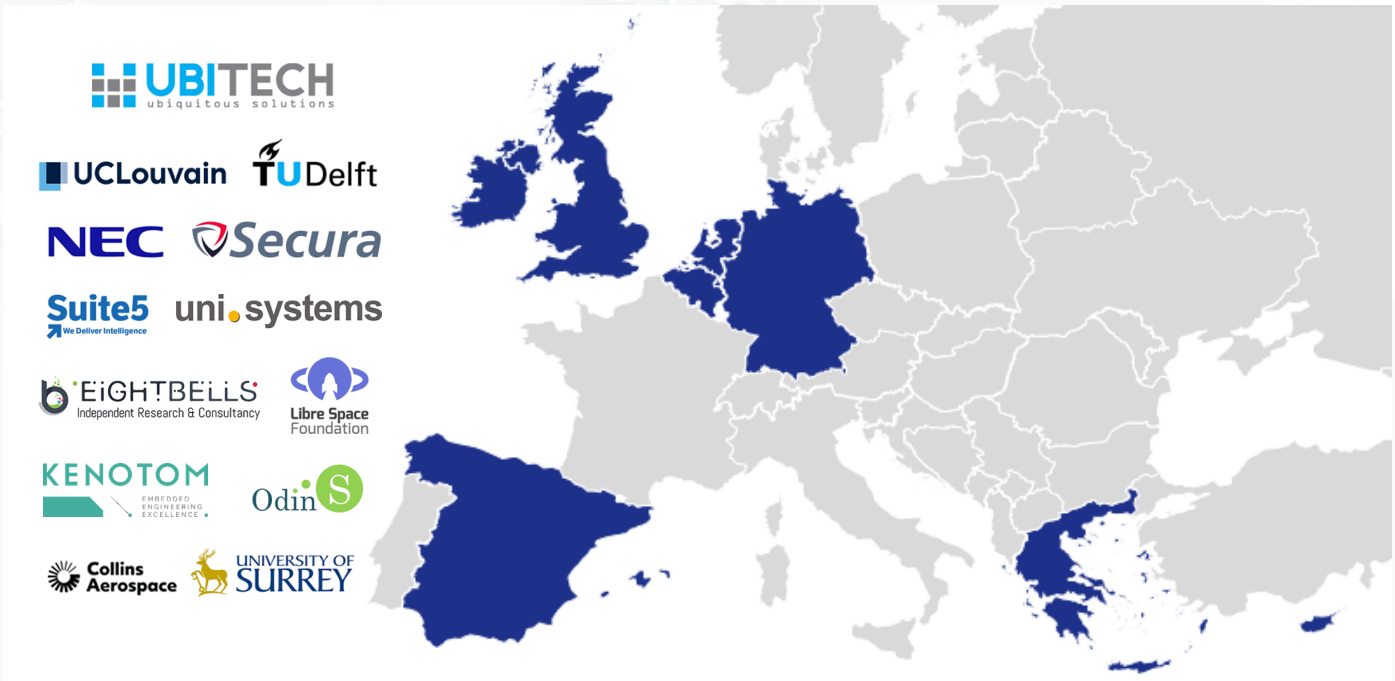
◊ Embedded software security analysis in REWIRE, by Sjors van den Elzen, SECURA
◊ Secure Remote Computation and Trusted Execution Environments, by Javier Vicente, NEC
◊ Blockchain, Oracles, and Trust in Project REWIRE, by Dr. Kaitai Liang, TUD
◊ AI-based Misbehavior detection in IoT environments, By Spiros Kousouris, SUITE5
◊ The continuous integration and development process of REWIRE towards the assurance of the secure lifecycle of IoT devices, by Ilias Aliferis, UNISYS
◊ Data Format Fusion Mechanism, by Konstantina Papachristopoulou, 8BELLS

Funded by the European Union

At a glance

Rewire consortium

REWIRE brings together 13 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