SECURE PLATFORM FOR ICT SYSTEMS ROOTED AT THE SILICON MANUFACTURING PROCESS (SPIRS)

Blog 5: WP6 Outcomes

In the rapidly evolving landscape of Industry 4.0 and 5G networks, security and accountability are of paramount importance. As systems become more interconnected and data-intensive, the risks associated with data breaches, unauthorized access, and security threats increase exponentially. The SPIRS platform, based on a RISC-V architecture secured with the Keystone Trusted Execution Environment (TEE) and a customized Hardware Root-of-Trust (HW RoT), addresses these challenges by offering a secure solution.

After designing and developing the needed parts and components of the system, one of the most crucial phases of the SPIRS project was the validation of the platform, which is the main goal of WP6. The validation allows to ensure that the security solutions developed were practical, reliable, and actually useful across various real-world applications. This blog-post covers the main outcomes of WP6 and their relationship with other work packages.

The first deliverable of WP6 focused on analysing the Industry 4.0 and 5G Network scenarios to identify potential security vulnerabilities and to establish the necessary requirements. This analysis helped the definition of the specifications for a customized SPIRS implementation. These specifications also served as input for other key work packages, including WP3 and WP4. Additionally, the deliverable involved the definition of a detailed plan to guide the overall validation activities, ensuring a structured and thorough approach to testing the security solution across the identified use cases.

In the 5G use case (Figure 1), SPIRS is deployed within a Public Network-integrated Non-Public Network (PNI-NPN) to secure wireless connectivity for enterprise devices such as IoT systems and robots. Leveraging a zero-trust approach, the platform establishes an end-to-end IPsec overlay between two SPIRS Trusted Network Edge Devices (TNEDs), ensuring secure communication and data protection across both local enterprise networks and remote monitoring through the 5G core infrastructure.

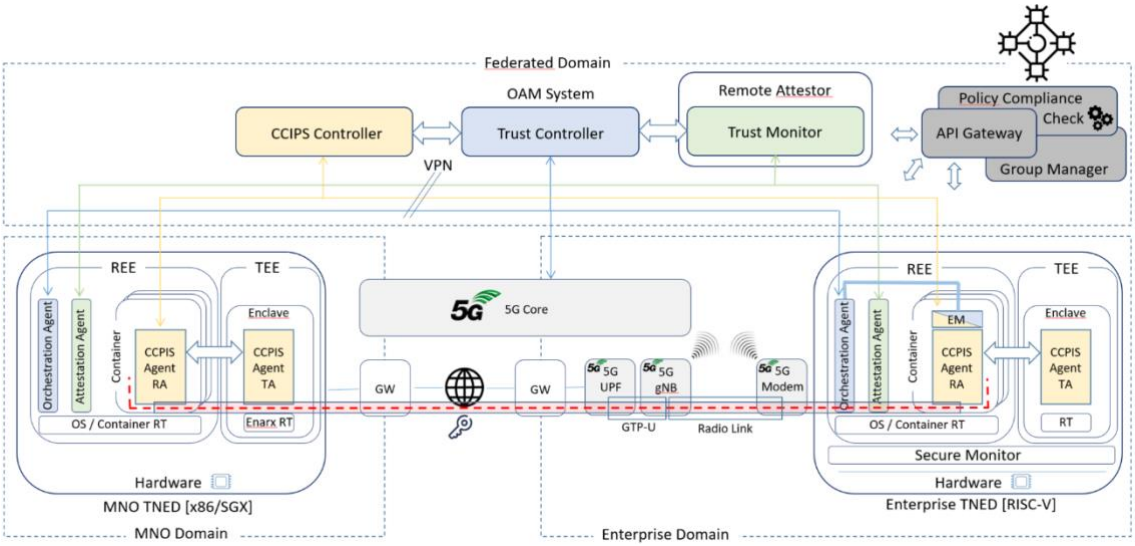

Figure 1 – 5G setup for the validation of SPIRS zero-trust enablers

In the second scenario (Figure 2), the attestation and privacy enhancement mechanisms together the SPIRS TEE and HW RoT enable to produce a secure network gateway for Industry 4.0 IoT devices. Those validated are the Trust in Manufacturing Machine, where the SPIRS platform is installed at the physical machine of a production line and protects the data for the MES Server, and the Secure Firmware Exchange that protects the firmware produced by customers and monitor the accesses during the final stage of the production.

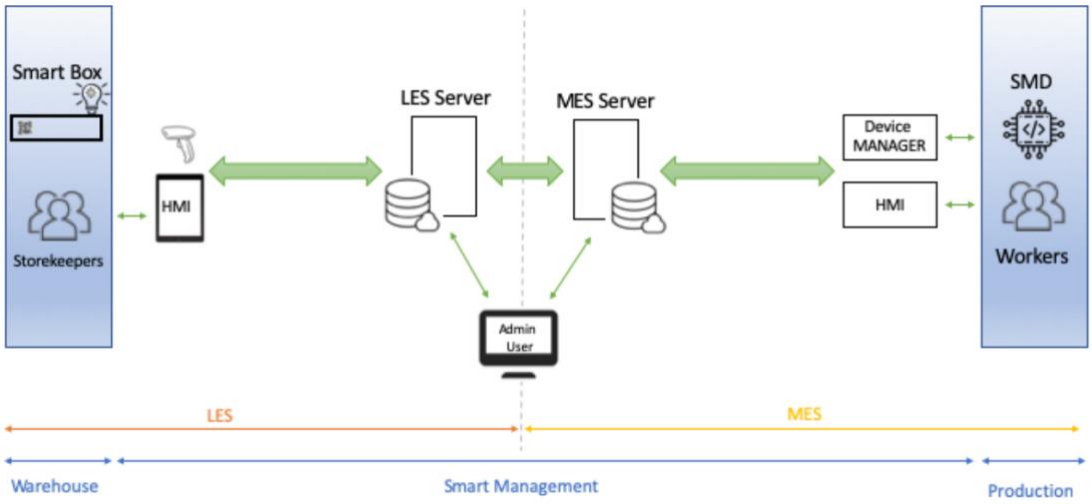

Figure 2 – Schematics of the Industry 4.0 use case in SPIRS

The second deliverable of WP6 describes in detail the PoC of the SPIRS governance scheme in the Industry 4.0 and 5G Network scenarios. The SPIRS governance scheme is mainly determined by the privacy respectful identity management developed in the project and the Distributed Ledger Technology (DLT) protocols for the gathering and recording of activity and security events. SPIRS supports two different options for DLT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952622

that are accessible through the API Gateway: the IOTA Tangle and Hyperledger fabric. For identity management, the group signatures library developed in SPIRS allows the definition of operational roles related to the Industry 4.0 and 5G Network use cases. This deliverable also provides the results of the validation activities of the SPIRS platform following its integration in the two real-world use cases.

The validation phase was essential in demonstrating that SPIRS is not just a theoretical or lab-based solution but one that can be placed in real-world environments, proving its adaptability. This is particularly important as both Industry 4.0 and 5G environments are highly dynamic, with new devices and processes newly created. The ability of the SPIRS platform to adapt to these changing environments was a critical outcome of the validation process, together with the enhancement to the security of the processes involved in the various use cases.

Lead partner of WP6: LINKS

Author: Alberto Carelli (LINKS)

Submission date: 16/09/2024

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952622