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

Blog 2: WP3 Outcomes

The main goal of WP3 is the design of SPIRS TEE (Trusted Execution Environment). This allows creating trusted computing applications in the platform. At the same time, the TEE must rely on other components developed in SPIRS to provide its security assurances. This blogplost covers the main outcomes of WP3 and their relationship with other work packages.

SPIRS TEE is based on the Keystone framework for creating custom TEE for RISC-V-based systems. The first deliverable of WP3 was set in the first six months of the project. It defines the requirements of SPIRS TEE and sets the API that will be implemented to be used to communicate between the security domains in the systems (i.e., trusted, and untrusted world). We decided to follow the GlobalPlatform TEE API specification to support this. These APIs are used in the ARM ecosystem; therefore, this adoption reduces the gap between them, allowing easier porting to established platforms like OP-TEE when they become available for RISC-V.

The second deliverable of WP3 holds more tangible results. It has the first version of the TEE with the implementation of the GlobalPlatform TEE API subset used in the project. In addition to a Keystone-based TEE tailored for SPIRS our team provided an application development framework that simplifies and unifies the development of untrusted and trusted applications. It also simplifies the integration and deployment of the software images of the platform.

OK, it is time to zoom-out for a bit, the TEE features described so far would be security-wise limited if the platform cannot be attested. This process starts at the booting phase therefore in WP3 we developed a measured boot implemented on top of the DICE specification. DICE allows to derive HW and SW bounded identifiers. This leverages on the PUF (Physically Unclonable Function) developed in WP2 to derive HW-bounded secrets allowing to measure for attesting the integrity of the platform where TEE applications run.

Following the execution stack, to attest the Linux runtime environment we used existing solutions based on a TPM (Trusted Platform Module). For this, in the framework of WP3, we developed a TPM as a Trusted Application that lives inside the TEE (i.e., firmware TPM, fTPM). The fTPM consumes DICE boot measurements securely. The adoption of core technologies, like a TPM, for the attestation of the Linux runtime on the SPIRS platform enables the use of established technologies for implementing the remote attestation protocols developed in WP3.

Two other contributions are developed in WP3: the implementation of an easy-to-use group signatures library; the design and deployment of TEE based blockchain protocols for authentication, authorization, audit, and accountability (AAAA). The libgroupsig library has been developed as a fork from IBM libgroupsig library, which is an extension of a former version of the libgroupsig library implemented by part of the GiCP team. In SPIRS we have adapted legacy versions of some of the group signatures included in IBM libgroupsig. The software interface has been changed according to the needs of the use cases in SPIRS, which also favors its use by external users.

Intensive work has been carried out to enable the use of libgroupsig inside SPIRS TEE environment. This task has been an important set of coding sprints based on the limitations of the TEE environment. As result of the work carried out until this moment, libgroupsig is offered as an open-source library to support the implementation of group signatures with support to a variety of control policies with respect to identity traceability and linkability in coherence with privacy protection goals. In SPIRS, we are designing blockchain protocols to record security events from network monitoring and remote attestation protocols. In fact, the libgroupsig library not only allows privacy protection of users but also makes it possible to implement fair anonymity by means of privacy-respective traceable group signatures. In SPIRS, the GiCP team has been working on the design of AAAA blockchain protocols in 5G and Industry 4.0. Specifically, we have created a privacy-respectful layer to be used by remote attestation protocols and the rest of Trusted Applications deployed using SPIRS TEE. On this basis, we have designed blockchain protocols to bear the deployment of reliable systems using SPIRS RISC-V TEE.

Lead partner of WP3: TAU

Author: Alejandro Cabrera Aldaya (TAU; Tampere University)

Submission date: 24/04/2024

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