Politecnico di Torino

1859

Finanziato dall'Unione europea
NextGenerationEU

COMPUTER AND CONTROL ENGINEERING

Security of cyber-physical systems

Funded By	FONDAZIONE LINKS - LEADING INNOVATION & KNOWLEDGE FOR SOCIETY [P.iva/CF:11904960017] Ministero dell'Università e della Ricerca - MUR [P.iva/CF:96446770586]
Supervisor	LIOY ANTONIO - antonio.lioy@polito.it
Contact	Andrea Vesco (andrea.vesco@linksfoundation.com)
Context of the research activity	Modern ICT infrastructures – with edge/fog computing, personal devices, and IoT – can control physical systems (e.g. vehicle driving assistance, efficient energy management, home automation, personal healthcare devices) giving rise to the so-called cyber-physical systems (CPS). This calls for very strong security because an attack towards a CPS component may result not only in a logical error but also in a physical damage, up to harm to human beings. The research will investigate various security aspects of CPS, such as device identity, software integrity, trusted execution of applications, access control, and communication security, exploiting various advanced techniques , included (but not limited to) blockchain, self-sovereign identity, post-quantum cryptography, secure hardware elements (TPM, crypto engines), and artificial intelligence for attack detection and reaction. The final objective is to build a secure ecosystem for CPS components and their management.
	The main objectives of the research activity are the following ones. 1. Identify, design, and implement solutions for device identity, evaluating centralized (PKI) and decentralized (blockchain) solutions as well as self-sovereign identity techniques for minimal disclosure of information in access control. 2. Evaluate the required hardware support to ensure trusted execution of applications on nodes with limited computational capabilities. 3. Implement a testbed to demonstrate the feasibility and effectiveness of a secure ecosystem for CPS that includes strong identity, secure communications, and integrity monitoring with trusted-computing and AI-based techniques. The first year will be spent studying the existing technologies for device identity (PKI, blockchian, self-sovereign-identity) and secure/trusted

Objectives	execution (Intel TXT and SGX, the Trusted Computing platform, and the ARM TrustZone). The PhD student will also investigate AI-based techniques to detect anomalies, for application to attack detection. During this year, the student should also follow most of the mandatory courses for the PhD and submit at least one conference paper. During the second year, the PhD student will design an optimised solution for protection of CPS that includes identity, hardware-based secure/trusted execution, protected communications, and AI-based anomaly detection. The application domain should be oriented to critical infrastructures or systems, such as power distribution, automotive, traffic management. At the end of the second year, the student should have started preparing a journal publication on the topic and submit at least another conference paper. Finally, the third year will be devoted to the implementation and evaluation of the proposed solution, compared with the existing ones. At the end of this final year, a publication in a high-impact journal shall be achieved. All the activities will performed in coordination with LINKS Foundation and its industrial customers.

Skills and competencies for the development of the activity	(mandatory) Cybersecurity (preferred) Cloud computing, Embedded systems, AI/ML