ARTIFICIAL INTELLIGENCE

PNRR - AI-Driven Approaches for Enhanced Hardware and Operating System Security

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019]
Supervisor	DI CARLO STEFANO - stefano.dicarlo@polito.it
Contact	SAVINO ALESSANDRO - alessandro.savino@polito.it DI CARLO STEFANO - stefano.dicarlo@polito.it
Context of the research activity	Utilization of artificial intelligence (AI) techniques to enhance security in both hardware and operating system (OS) domains. Progetto finanziato nell'ambito del PNRR. PNRRM4C2, Investimento1.3-Avvison.341del15/03/2022-PE0000014Security and Rights in the CyberSpace (SERICS) - CUP E13C22001850001
Objectives	This abstract presents a research proposal on the utilization of artificial intelligence (AI) techniques to enhance security in both hardware and operating system (OS) domains. With the continuous growth of cyber threats, there is an urgent need to develop proactive and intelligent security mechanisms. This research aims to leverage AI algorithms and machine learning models to detect and mitigate security vulnerabilities in hardware and OS components. By analyzing system-level data, behavior patterns, and anomaly detection, the proposed framework seeks to identify and respond to potential threats in real time. The research will focus on exploring AI-driven solutions for hardware security, such as side-channel attacks, hardware Trojans, and fault injections, as well as OS security challenges, including malware detection, intrusion detection, and privilege escalation. The development of AI-based techniques will involve the integration of machine learning algorithms, data-driven modeling, and predictive analytics to enhance the security posture of hardware and OS environments. To validate the effectiveness of the proposed approaches, extensive experimental evaluations will be conducted using diverse datasets and real-world scenarios. The performance impact, scalability, and adaptability of the AI-driven security framework will be assessed, ensuring practical applicability

	across different hardware architectures and operating systems. The expected outcome of this research is to contribute to the advancement of hardware and OS security by harnessing the power of AI. The developed techniques will aid in proactively identifying and mitigating security threats, reducing the risk of system compromises, and fortifying the resilience of both hardware and operating system components.

Skills and competencies for the development of the activity	Candidate must possess a combination of technical skills, knowledge, and research capabilities: - Strong understanding of Real-Time Embedded systems - Proficiency in hardware and OS security concepts - Solid knowledge of AI and anomaly detection techniques - Proficiency in HDL and experience with C/C++, Rust, and Python are required. - Ability to read and understand the literature. - Effective English communication skills, both written and verbal