PhD Candidate full name: Tadeu Augusto Leite Freitas

Dissertation Title: SkyNet: Towards a Dynamic and Adaptive Intrusion Tolerant System

Date: 08/07/2026 08:44:00

Location: University of Porto | Faculty of Sciences | Department of Computer Science | FC6 029

Higher Education Institution: University of Porto

Abstract or Public Summary: The thesis presents SkyNet, a novel architecture for adaptive, dynamic ITS designed to withstand and mitigate increasingly sophisticated, multi-domain cyber threats by integrating concepts from cybersecurity, AI, and distributed systems. Addressing the limitations of traditional perimeter defenses and conventional BFT protocols, SkyNet acknowledges the inevitability of breaches, particularly from APTs, and focuses on maintaining system resilience through diversity, redundancy, proactive recovery, and dynamic reconfiguration.The architecture distinguishes between a trusted, secure Control Plane—which manages risk assessment, configuration, and orchestration using AI-driven modules such as the HAL risk manager—and an untrusted Execution Plane exposed to adversaries. The thesis elaborates on SkyNet's integration of real-time threat intelligence gathering (via the VExHK module), ML-based vulnerability scoring, and FL-enhanced intrusion detection to optimize system configurations for both minimal security risk and maximal resilience to correlated compromises. Complementary systems such as EVSOAR, which leverages EV charging infrastructure for secure, low-latency intrusion detection and response, and LegionITS, a federated ITS architecture enabling privacy-preserving cyberthreat intelligence sharing across organizations, demonstrate the practical applicability and scalability of the proposed framework. Experimental evaluations highlight HAL's superiority in reducing risk exposure windows through automated, predictive vulnerability scoring and risk assessment. In contrast, EVSOAR's network evaluations demonstrate significant improvements in latency, throughput, and detection efficacy compared to traditional vehicle security operations. The federated approach of LegionITS addresses privacy, scalability, and trust challenges inherent in multi-organization collaboration. The thesis argues that a multidisciplinary design integrating BFT consensus protocols, AI-driven adaptive risk management, privacy-preserving federated collaboration, and automated orchestration forms a powerful basis for next-generation resilient cybersecurity architectures, capable of protecting critical infrastructures and complex systems against evolving cyber threats.

Doctoral Programme: Doctoral Program in Computer Science

Research Centre: CRACS

Principal Supervisor at INESC TEC: Manuel Eduardo Correia

Additional Supervisor: Rolando Martins (University of Porto)

Scientific Domain: Computer Science and Engineering