PhD Candidate full name:

André Nuno de Pinho Tavares Gurgo e Cirne

Dissertation Title: Identity and Trust based on Hardware for IoT

Date: 11/03/2026 14:30

Location: UP | FCUP | DCC | FC6 0.29

Higher Education Institution: University of Porto

Doctoral Programme - Doctoral Program in Computer Science (FCUP)

Abstract or Public Summary: As the number of Internet of Things (IoT) devices continues to grow exponentially, the question of how to establish and maintain trust among billions of interconnected objects has become a central challenge in modern cybersecurity. At the core of this challenge lies the notion of device identity: without a secure and verifiable identity, it is nearly impossible to determine whether a device can be trusted. Yet, implementing robust identity mechanisms in IoT environments is far from trivial. These devices are typically constrained by limited computational and energy resources, and are often deployed in remote, uncontrolled, or physically exposed locations, conditions that make them especially vulnerable to both software and hardware-based attacks. This thesis explores the fundamental relationship between identity, trust, and hardware in the context of IoT. While hardware is frequently regarded as a bottleneck that limits the feasibility of strong security solutions, our work investigates the opposite perspective: can hardware itself become the enabler of secure and efficient identity mechanisms? To address this question, we begin by examining the current landscape of hardware based identity systems and identifying the main challenges that arise from hardware security limitations. We then conduct an experimental case study on a real device to illustrate how its identity can be compromised in practice and to evaluate potential mitigation strategies. Building upon these insights, we propose a novel runtime attestation frame work that leverages a recently introduced hardware feature, Pointer Authentication and Branch Target Identification (PACBTI). In parallel, we analyze the security implications and practical trade-offs introduced by this feature. Our findings reveal that several existing hardware-based technologies, such as Trusted Execution Environment (TEE) and PACBTI, are already present in many commodity devices and can be effectively leveraged to overcome the resource constraints that traditionally hinder the deployment of secure identity and trust mechanisms in IoT. However, despite this promising potential, a number of architectural, usability, and standardization barriers continue to limit their widespread adoption. By highlighting these challenges and opportunities, this work contributes to a deeper understanding of how hardware can evolve from being a limitation to becoming a cornerstone of secure identity in the future of IoT.

Principal Supervisor at INESC TEC: João Resende

Additional Supervisor: Patrícia Raquel Vieira Sousa (INESCTEC - research collaborator); Luís Antunes (University of Porto)

Scientific Domain: [Computer Science and Engineering]

Keywords: identity; trust; hardware-security; IoT