



José Areia

Leiria, Portugal | jose.apareia@gmail.com | +351 965 887 768 |  LinkedIn |  GitHub

Skills

Programming Languages: Python, Java, JavaScript, PHP, Lua, Perl, Haskell

Security Tools: Wireshark, Metasploit, Burp Suite, Nessus, Nmap, Wazuh

Security Practices: Risk Analysis, Vulnerability Assessment, Penetration Testing, Incident Response

Technologies and Frameworks: Linux, Docker, Git, PyTorch, TensorFlow, Scikit-Learn

Work Experience

Research Fellow, Computer Science and Communication Research Centre Feb 2022 – Present

- Developed IoT simulations for smart cities and medical applications, including attack scenarios and traffic analysis.
- Built DNN, ML, and generative models for intrusion detection and adversarial sample generation.
- Researched vulnerabilities in ML models, focusing on privacy, security, and robustness against attacks.
- Published peer-reviewed research articles showcasing key findings, methodologies, and openly available datasets.

Invited Assistant Professor, Polytechnic University of Leiria Sept 2023 – Aug 2025

- Teach in the Short Cycle Cybersecurity and Computer Networks programme.

Full Stack Developer, Estudar Portugal Feb 2019 – Feb 2021

- Developed a Laravel web application for HR, document, and finance management.
- Designed the application's data model and graphical interfaces.
- Managed and maintained web and email servers.
- Implemented a Scrumban methodology to improve in-company work organisation.

Selected Project

Multi-Objective Adversarial Generative Model

- Designed a multi-objective generative architecture to craft adversarial samples targeting computer vision models.
- Achieved up to 91% misclassification across multiple models with minimal perturbations.
- Evaluated sample quality using state-of-the-art metrics such as LPIPS and FID.
- Integrated with adversarial training, lowering fooling rates of target models by up to 73%.

Education

Polytechnic University of Leiria, MSc in Cybersecurity and Digital Forensics Sept 2023 – Present

- Grade: 18/20

Polytechnic University of Leiria, BS in Computer Engineering Sept 2020 – Jul 2023

- Grade: 16/20

Polytechnic University of Leiria, TeSP in Web Development and Multimedia Sept 2018 – Jul 2020

- Grade: 20/20 - Awarded Merit Student

Publications

Balancing Image Quality and Attack in Multi-Objective Adversarial Image Generation Aug 2025

José Areia, Leonel Santos and Rogério Luís de C. Costa

ACM KDD International Conference on Knowledge Discovery and Data Mining

Fooling Rate and Perceptual Similarity: A Study on DCGAN-based Adversarial Attacks Aug 2025

José Areia, Leonel Santos and Rogério Luís de C. Costa

20th International Conference on Availability, Reliability and Security

IoMT-TrafficData: Dataset and Tools for Benchmarking Intrusion Detection in IoMT Aug 2024

José Areia, Ivo Afonso Bispo, Leonel Santos and Rogério Luís de C. Costa

IEEE Access, 12, 115370-115385

Dvorak: A Browser Credential Dumping Malware Jul 2024

José Areia, Bruno Santos and Mário Antunes

21st International Conference on Security and Cryptography