José Flora

linkedin.com/in/jeflora | jeflora.github.io | github.com/jeflora

EDUCATION

University of Coimbra	Coimbra, Portugal
PhD in Informatics Engineering (Architectures, Networks, and Cybersecurity)	*Sep. 2019– EXP: Sep. 2024*
University of Coimbra	Coimbra, Portugal
Master in Informatics Security (Cybersecurity)	*Sep. 2017– Sep. 2019*
University of Coimbra	Coimbra, Portugal
Bachelor in Informatics Engineering	*Sep. 2014– June 2017*

TECHNICAL SKILLS

Languages: English (C1 - Cambridge CAE), Portuguese (Native)
Processes: Code Review, System Design, Threat Modeling, Testing, Static Analysis, Fault Injection, Vulnerability Injection and Attack Injection, Benchmarking
Programming Languages: Java, Python, C/C++, SQL, JavaScript, HTML/CSS
Databases: MySQL, MariaDB, PostgreSQL, MongoDB
Frameworks: Flask, FastAPI, Node.js
Developer Tools: Git, Docker, LXC, Kubernetes, Vagrant, PyCharm, IntelliJ, Eclipse
Libraries: pandas, NumPy, Matplotlib

EXPERIENCE

Security Researcher @ CISUC Coimbra, Portugal / Remote | June 2017– Present

Publications: *2 journal articles, 7 conference papers $\simeq$ 75 cit. | scholar.google.com/citations?user=utdIQnwAAAAJ*
- Identify, understand, and validate research gaps to advance knowledge; Define, design, and conduct experiments to collect and analyze data; Analyze and interpret results and draw inferences and conclusions
- Write reports and research papers and present findings at conferences; Collaborate with academic and industry partners on R&D projects
- Conduct a study on fault tolerance of microservices and orchestrators; Proposed benchmark and dataset to evaluate IDSs for microservices; Developed end-to-end IDS for microservices using CI/CD pipelines
- (Master Thesis Co-advisor) Advised and trained two master students working on intrusion detection for microservice applications; Supervised three MSc students in a one-semester research project

Teaching Assistant @ Dep. of Informatics Engineering, UC Coimbra, Portugal | Sep. 2020– Aug. 2023

Courses: *Cyber Security Assessment and Management, Operating Systems, Databases, Informatics Systems*
- Lectured practical (and occasionally theoretical) classes for masters and bachelors level students.
- Topics such as: Threat Modeling; Risk Management; Attack Injection and Vulnerability Assessment; Benchmarking; Attack Surface; PostgreSQL; Concurrency; Synchronization; Memory Management; C and Java
- Prepare, present, assist, and grade students' practical assignments
- Mentored two master students' independent studies work part of masters degree in topics related to evaluation of AI models in detecting cyber attacks and development of capture the flag (CTF) platforms
- Invited Classes on Trusted Execution Environments with practical tutorial on Intel SGX (https://github.com/jeflora/sgx-demo-app)

Member of Security Benchmarking WG @ SPEC RG Remote | Jan. 2020 – Present
- Research collaborations on Security and Benchmarking topics: hypervisors, hypercalls, intrusion detection, malware, containers, microservices
- Publication in JSS Journal benefited from discussions and brainstorming sessions at SPEC RG meetings
- Member since Jan 2020; Secretary and Release Manager since Jan 2021

PROJECTS

μSherlock | *Python, FastAPI, Redis, Kubernetes, sysdig, Docker, Git, Next.js, Typer* Dec. 2023– Present
https://jeflora.github.io/sherlock | ***Team:*** *José Flora, Nuno Antunes*
- End-to-end IDS for microservices using CI/CD pipelines

μDetector | *Python, Flask, Redis, Jinja2, sysdig, Kubernetes, KubeEdge, Git* Sep. 2021– July 2022
https://micro-sec.github.io/detector | ***Team:*** *Miguel Teixeira, Paulo Gonçalves, José Flora, Nuno Antunes*
- Proof-of-Concept Intrusion Detection for Microservices

Adaptive, Intelligent and Distributed Assurance | *International Research Project* May 2020– Sep. 2023
https://aida.inesctec.pt | ***Consortium:*** *Mobileum, INESC TEC, University of Coimbra, Carnegie Mellon University (CMU)*
- International CMU Portugal R&D Project with academic and industry partners; Work focused on ensuring security and privacy for microservice applications (Activity 4)