David Araújo

Cybersecurity Master's Student and Graduate Researcher

david2araujo5@proton.me | davidjosearaujo.dev

Education

University of Aveiro — Aveiro, PT
M.S in Cybersecurity — 09/2023 - Present
B.Eng. in Computer Science and Telematics — 09/2018 - 07/2023

Experience

Graduate Student Researcher — 09/2023 - Present
Instituto de Telecomunicações

- Improve non-5G devices authentication and authorization (AA) mechanisms and support for legacy device in 5G networks, as its functions require devices to have 5G credentials.
- Stress testing and development of resilience improvements of TeraFlowSDN cloud-native architecture.

Undergraduate Student Researcher — 11/2022 - 07/2023
Instituto de Telecomunicações

- Inserted in the FireTec project, my position was created with the intent of adding CAP (Common Alert Protocol) communication support to the existing infrastructure. (see 1)

Skills

Programming Languages: Go, Python, Rust, JavaScript, Java, C, Zig, Bash
Tools and Frameworks: Git, Ansible, Terraform, Docker, Vagrant, Kubernetes, MSSQL, SQL, GraphQL, AWS, Google Cloud, Prometheus, Grafana
Cybersecurity Skills: GRC, Risk Assessment, IAM Management, Threat Modelling, IS Auditing, SSDLC, SAST, DAST, Vulnerability Management, API Penetration Testing, Threat Hunting
Languages: Portuguese (native), English (proficient)

Projects

Reverse Engineering - PDF Manager Malicious Android Application — 2024

- Analysis of the PDF Reader File Manager application. This was developed with the intent of stealing data from Android users, as described in this article.

Flexible, Risk Aware Authentication System — 2024

- Design and implementation of an Identity Provider (IdP) using the OAuth 2.0 protocol, and three client services which use it for authentication and authorization.

Enhanced DES (E-DES) — 2023

- Implementation of a DES variant known as E-DES, using a 256-bit key, derived from a user-provided password and S-boxes derived from the key, instead of using fixed and known S-boxes.

Deterministic RSA key generation (D-RSA) — 2023

- Deterministic RSA key generation and implementation of a pseudo-random number generator and RSA key generator

Certifications

Blockchain Security Specialization, Infosec — 07/2024
Cyber Incident Response Specialization, Infosec — 07/2024
Cyber Threat Hunting Specialization, Infosec — 07/2024
Information Systems Auditing, Controls and Assurance, Hong Kong University — 07/2024
API Penetration Testing, APIsec University — 09/2023

Publications

1. **A Low-Cost Embedded System to Support Broadcasting Emergency Messages rough FM Radio Stations**
   M. Coelho; L. Santiago; D. Araújo; A. Navarro; N. B. Carvalho
   IEEE Embedded Systems Letters, vol. 16, no. 3, pp. 247-250, Sept. 2024