

Miguel Quaresma

LinkedIn Github Website/Blog

Email: miguelquaresma.w@gmail.com/a77049@alunos.uminho.pt

Education

- Currently enrolled in a Masters degree in **Cryptography and Information Security** and **Parallel and Distributed Computing** at Universidade do Minho, Braga (expected graduation date: June 2020); doing research in “Runtime verification framework using ARM TrustZone”
- Bachelors Degree in **Computer Engineering** at Universidade do Minho, Braga
- Fluent in Portuguese (native), English (Level B1 by Cambridge), Spanish (intermediate)
- **Relevant Coursework:** Cryptographic Technologies, Cryptographic Structures, Security Technology, Security Engineering, Advanced Computer Architectures, Parallel Computing Paradigms, Parallel Algorithms, Computer Systems Engineering, Algorithms and Data Structures

Professional Experience

Security Engineering Intern at Aptoide (July 2019 - September 2019)

Summer Internship during which I worked on a malware detection engine aimed at keeping Android malware from being released to the Aptoide App Store. The malware engine used Yara as to identify and classify malware samples via known malware patterns as well as Django and Celery for backend processing and API.

Software Engineering Intern at Closer Consulting (August 2018)

Summer internship during which I worked in a document management system for an insurance company, improving the front-end(in Angular 5) and developing the CRUD module for the back-end(in NodeJS) of that application. Furthermore I worked on an order management application, using Angular 5, Bootstrap and .NET to implement new features and fix existing bugs.

Relevant Projects

ARM Trusted Firmware: modified ARM Trusted Firmware to load a device specific certificate and encrypted signing key used by OPTEE to perform attestation services

OPTEE: forked OPTEE to implemented a mechanism aimed at providing attested computation services to Trusted Applications running in the Secure World

Cryptographic-Implementations: used Python to implement several cryptographic systems and attacks on some of those systems

MellonFS: used C and libfuse to develop a userspace filesystem that improves access control by authenticating users via an OTP sent to the user's email address each time a file is accessed. Python and Flask were also used to develop a web front end for the file system authentication mechanism

Hard Skills

Operating Systems

Experience using both *macOS* and *Linux* environments for development and administration purposes.

Development

Development using Haskell, C/C++, Java, Javascript/Typescript, C#, Python, Jasmin, Assembly (x86 and ARM).

Performance focused development(tuning) using PAPI, OpenMP, OpenMPI and CUDA.

Use of **front-end frameworks** such as Bootstrap and Angular and **back-end frameworks** such as NodeJS, Django, Celery, Redis and .NET.

Formal verification of cryptographic primitives using Easycrypt.

Experience in **database technologies** such as MySQL, SQL Server, Neo4j and MongoDB.

Fluent in **markup languages** such as Markdown, HTML, XML and \LaTeX .

Use of **security tools** such as Yara, Androguard.