Miguel Quaresma

LinkedIn Github Website/Blog
Email: miguelquaresma.w@gmail.com

Professional Experience

Cybersecurity Analyst at Goldman Sachs (August 2020 - now)
Cybersecurity Analyst at Goldman Sachs performing security assessments and penetration tests of applications.

Security Engineering Intern at Aptoide (July 2019 - September 2019)
Developed a malware detection engine for integration with the app release pipeline of the Aptoide App Store, using Yara to identify and classify malware samples. Applied several optimization techinques, which resulted in a 25% performance gain in analysis time.

Software Engineering Intern at Closer Consulting (August 2018)
Worked in a document management system for an insurance company, improving the front-end (Angular) and developing the CRUD module for the back-end (NodeJS) of that application. Also worked on an order management application, using Angular 5, Bootstrap and .NET to implement new features and fix existing bugs.

Education

- MSc in **Cryptography and Information Security** and **Parallel and Distribuited Computing** at Universidade do Minho, Braga; Thesis: "TrustZone based Attestation in Secure Runtime Verification in Embedded Systems", Grade 18/20 (September 2018 - July 2020)
- Bachelors Degree in **Computer Engineering** at Universidade do Minho, Braga (September 2015 - June 2018)
- 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

Relevant Projects

High-speed Certified Crypto: developed a fast and certified implementation of Keccak (SHA-3) using Jasmin and Easycrypt
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
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 implement a mechanism aimed at providing attested computation services to Trusted Applications running in the Secure World

Hard Skills

Development

Development using Haskell, C/C++, Java, Python, Jasmin, Assembly (x86 and ARM), Rust.
Formal verification of cryptographic primitives using Easycrypt.
Performance focused development using PAPI, OpenMP, OpenMPI and CUDA.
Use of **security tools** such as Yara, Androguard.
Use of **back-end frameworks** such as NodeJS, DJango, Celery, Redis and **.NET**.
Experience in **database technologies** such as MySQL, SQL Server, Neo4j and MongoDB.
Fluent in **markup languages** such as Markdown, HTML, XML and LaTeX.

Operating Systems

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