Miguel Quaresma

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

Professional Experience

Max Planck Institute for Security and Privacy - PhD Researcher (February 2021 - now)
PhD Researcher working on high speed high assurance cryptography, supervised by Peter Schwabe and Gilles Barthe
Goldman Sachs - Cybersecurity Analyst (August 2020 - January 2021)
Cybersecurity analyst responsible for penetration tests, cloud security, security research
Aptoide - Security Engineering Intern (July 2019 - September 2019)
Malware detection engine development
Closer Consulting - Software Engineering Intern (August 2018)
Fullstack development in NodeJS, .NET, Bootstrap and Angular

Education

- **MSc in Computer Engineering** at Universidade do Minho (September 2018 - July 2020)

  Specializations: *Cryptography and Information Security* and *Parallel and Distributed Computing*

  Thesis: "TrustZone based Attestation in Secure Runtime Verification in Embedded Systems", supervised by José Bacelar Almeida, Grade 18/20

- **BS in Computer Engineering** at Universidade do Minho, Braga (September 2015 - June 2018)

- **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

- Fluent in Portuguese (native), English (Level B1 by Cambridge), Spanish (intermediate)

Relevant Projects

High-speed Certified Crypto: fast and certified implementation of Keccak (SHA-3) using Jasmin and Easycrypt
ARM Trusted Firmware: ARM Trusted Firmware fork with support for attestation services via device specific certificate and encrypted signing key loaded at boot time
OPTEE: OPTEE fork with attested computation capability for Trusted Applications running in the Secure World
MellonFS: userspace filesystem with improved access control authentication via OTP

Hard Skills

- **Development**: Haskell, C/C++, Java, Python, Jasmin, Assembly (x86 and ARM), Rust
- **Formal verification:** of cryptographic primitives using Easycrypt
- **Performance analysis/Profilling:** PAPI, OpenMP, OpenMPI and CUDA
- **Security tools:** Yara, Androguard, BurpSuite
- **Back-end frameworks:** NodeJS, DJango, Celery, Redis and .NET
- **Database technologies:** MySQL, SQL Server, PostgreSQL, Neo4j and MongoDB
- **Markup languages:** Markdown, HTML, XML and LaTeX

Non Academic Interests

- Cycling, Swimming and (Trail-)Running
- Travel