Andrea Francesco Iuorio

Via Paolo Paruta 29, Milan, Italy | af.iuorio.eu | +393478821417 | andrea@iuorio.eu

EDUCATION

UNIVERSITÀ DEGLI STUDI DI MILANO

MSc. in Computer Science
February 2018 | Milan, IT
Final Score: 101 / 110

UNIVERSITÀ DEGLI STUDI DI MILANO

BSc. in Computer Science
February 2015 | Milan, IT
Final Score: 102 / 110

SKILLS

SOFTWARE DEV. INTERESTS

Cryptography • Computer security
Compilers • Virtual machines
Reverse Engineering • GPGPU
Multithreaded programming
Kubernetes • CI/CD

SOFTWARE DEV. SKILLS

Highly proficient in low-level programming:
C • Assembly X86 • JVM Bytecode
Proficient in object-oriented programming:
Java • C# • Python
Proficient in functional programming:
OCaml • Scala • Erlang • F#
Knowledge of web programming:
Javascript • React • ionic

PERSONAL PROJECTS

panz-gb
An emulator for the Gameboy system developed in C + SDL 2.0

panz-crypto
A collection of cryptographic algorithms in C

LANGUAGES

Italian: Native
English: C1 (TOEFL 103 / 120)

LINKS

Github: **afiuorio**
LinkedIn: **afiuorio**

EXPERIENCE

WELLD

Junior Software Developer | Sep 2018 – current | Milan, IT

- Worked on a tool for the real time identification of outages in the national electrical grid (Java EE)
- Worked on a tool for helping electricians on their field work (Java, React)
- Worked on the operation center software for EV charging units (Java EE, OCPP 1.6/2.0, Kubernetes)
- Developed an Android and iOS application for configure and get informations from a smart home device (Angular 10, ionic)
- Worked on a ML-based virtual concierge for hotels (Java EE, Quarkus, React, terraform, AWS)

CLUB - UNIVERSITÀ DEGLI STUDI DI MILANO

Software Developer Intern | Sep 2016 – Feb 2018 | Milan, IT

- Worked on acceleration attacks for Key Derivation Functions on GPUs
- Developed a GPU-based, highly optimized password guesser in C and OpenCL

GOOGLE SUMMER OF CODE 2017

Student Mentor | Apr 2017 – Sep 2017 | Remote

- I mentored a GSOC student for the Chapel project, helping them to design and implement the Crypto module for the Chapel programming language

GOOGLE SUMMER OF CODE 2016

Software Developer | Apr 2016 – Sep 2016 | Remote

- Implemented a stack trace mechanism in the Chapel runtime (C)
- Partial ported the debug symbols generation of the Chapel LLVM compiler backend to LLVM 3.7

GOOGLE SUMMER OF CODE 2014

Software Developer | Apr 2014 – Sep 2014 | Remote

- Worked on SGen, the garbage collector used by the Mono runtime (C)
- Added support to partial mark support for array of references and reduced the number of locks in task stealing

THESIS

EXPLOITING SHA-1 WEAKNESSES FOR SPEED UP PBKDF2

Advisor: Prof. Andrea Visconti

- My MSc. thesis describes which impact several known and new weaknesses of SHA-1 and HMAC have on PBKDF2 in the context of GPU-based attacks.

PORTABLE AND MODULAR EXCEPTIONS IN NEVERLANG2

Advisor: Prof. Walter Cazzola

- My BSc. thesis describes the definition and implementation of a runtime and compiler library for machine-independent exception handling procedures.

PUBLICATIONS

- Iuorio, Andrea Francesco, and Andrea Visconti. "Understanding optimizations and measuring performances of PBKDF2." International Conference on Wireless Intelligent and Distributed Environment for Communication. Springer, Cham, 2018.

In compliance with the Italian legislative Decree no. 196 dated 30/06/2003, I hereby authorize you to use and process my personal details contained in this document.