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
Multithreaded programming • GPGPU
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 • Electron

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).
- Developed our internal CI/CD infrastructure (Docker, Sonarqube, Gitlab).
- 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).

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

- Mentored a GSOC student for the Chapel organitation.
- I closely followed the student, helping him to design and implement the Crypto module for the Chapel programming language.

GOOGLE SUMMER OF CODE 2016

Software Developer | Apr 2016 – Sep 2016 | Remote

- Worked on the C runtime used by the Chapel programming language.
- Implemented a stack trace mechanism in the Chapel runtime.
- 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.
- Added support to partial mark support for array of references and reduced the number of locks in task stealing.

ADAPT LAB - UNIVERSITÀ DEGLI STUDI DI MILANO

Software Developer Intern | Jan 2013 – Jun 2013 | Milan, IT

- Worked on the Neverlang2 Exception Library, a compiler and runtime library for exception handling developed in Java.

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, with a particular interest 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 the development of machine-independent exception handling procedures.