Andrea Francesco Iuorio

Via Raffaello 12, Vigevano (PV), Italy
afiuorio.github.io | +393478821417 | andreafrancesco.iuorio@gmail.com

EDUCATION

UNIVERSITÀ DEGLI STUDI DI MILANO

MSc. in Computer Science
February 2018 (expected)

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

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#

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

GOOGLE SUMMER OF CODE 2017

Student Mentor | Apr 2017 – Sep 2017

- 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.

CLUB - UNIVERSITÀ DEGLI STUDI DI MILANO

Software Developer Intern | Sep 2016 – Sep 2017 | Milan, IT

- Worked on Key Derivation Functions and their interaction with parallel architectures.
- Developed a GPU-based, highly optimized password guessing application in C and OpenCL.
- Helped on works about h264 video encryption and circuit minimization.

GOOGLE SUMMER OF CODE 2016

Software Developer | Apr 2016 – Sep 2016

- 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

- Worked on SGen, the garbage collector used by the Mono runtime.
- Added support to partial mark support for array of references.
- Reduced the number of locks in the task stealing code used by SGen threads.

ADAPT LAB - UNIVERSITÀ DEGLI STUDI DI MILANO

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

- Worked on NEL, the Neverlang2 Exception Library.
- NEL is a compiler and runtime library for exception handling developed in Java.
- Implemented an object-oriented language for the Java Virtual Machine.

THESIS

EXPLOITING SHA-1 WEAKNESSES FOR SPEED UP PBKDF2

Advisor: Prof. Andrea Visconti

- My MSc. thesis describes which impact several known and new algorithmic and implementation 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 the Neverlang2 Exception Library, a runtime and compiler library for making easier the development of machine-independent exception handling procedures.

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.