Andrea Fioraldi's Curriculum Vitae

[REDACTED] street, [REDACTED]
Pontinia, LT. 04014 Italy.

Phone: +39 [REDACTED]

email: andreafioraldi@gmail.com
blog: andreafioraldi.github.io
GITHUB: andreafioraldi
TWITTER: @andreafioraldi

Born: [REDACTED], 1996—[REDACTED], Italy
Nationality: Italian

Current position

MSc Student in Engineering in Computer Science, Sapienza University of Rome.

Areas of specialization

System and Software Security • Software Testing

Honors and Awards

2017 First place in Binary Analysis (ex aequo) at CyberChallenge.IT 17.
2017 Second place in Penetration Testing at CyberChallenge.IT 17.
2017 Third place with the Italian National Cybersecurity Team at European CyberSecurity Challenge (ECSC).
2018 Seventh place at DEF CON 26 CTF (World Finals) with the mHACKeroni team.
2018 First place at Chaos Communication Congress CTF with the mHACKeroni+KJC team.
2019 Fifth place at DEF CON 27 CTF (World Finals) with the mHACKeroni team.

MSc Degree

2020 I got a MSc Degree in Engineering in Computer Science at Sapienza University of Rome with a degree of 110/110 cum laude.
My thesis is "Program State Abstraction for Feedback-Driven Fuzz Testing using Likely Invariants".

BSc Degree

2018 I got a BSc Degree in Computer Engineering at Sapienza University of Rome with a degree of 110/110 cum laude.
My thesis is "Symbolic Execution and Debugging Synchronization", available on ResearchGate.

Relevant Projects

Organizations and Events

2017 Co-founder of TheRomanXploit (TRX) academic Capture The Flag team.

2018 Co-founder of the mHACKeroni joint Capture The Flag team.

2018 Founder of the DEF CON 11396 Rome, a group that meets every month to do talks on advanced security topics at Sapienza.

Software (excerpt)

2017 *Carbonara*, a malware research platform designed to recognize duplicated functions between binaries at scale and speed-up the static malware analysis process.

2018 *angrdbg*, an abstract library used to implement synchronization between a concrete execution environment (tipically a debugger) and the angr symbolic execution engine.

2018 *IDAngr*, an IDA Pro debugger plugin that implements the angrdbg API in IDA with an user-friendly GUI.

2018 *angrgdb*, create an angr state from the current GDB state on top of angrdbg.

2019 *AFL++*, AFLplusplus is the daughter of the American Fuzzy Lop fuzzer and was created initially to incorporate all the best features developed in the years for the fuzzers in the AFL family and not merged in AFL.

2019 *frida-fuzzer*, an injectable fuzzer based on Frida that enables in-process fuzzing of Android/iOS APIs.

2020 *QEMU-AddressSanitizer*, QASan is a custom QEMU 3.1.1 that detects memory errors in the guest using AddressSanitizer.

Research Interests

My main interest is Software Testing for security, both with source code and binary-only. I'm comfortable with techniques such as Feedback-driven Fuzzing, Symbolic Execution, Dynamic Binary Instrumentation, Taint Tracking and more.
Currently I am researching new methodologies to overcome roadblocks in Fuzzing.
I am interested also in vulnerability auditing, binary exploitation and malware analysis as possible side topics of my research.
I am an enthusiat about Programming Languages. I built several educational programming languages both for my education and for the education of the young teammates of the TRX team about interpreters vulnerabilities and exploitation.

Publications

Academic

2020 Fioraldi Andrea and D'Elia Daniele Cono and Coppa Emilio, *WEIZZ: Automatic Grey-box Fuzzing for Structured Binary Formats* in Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis.

2020 Andrea Fioraldi, Dominik Maier, Heiko Eißfeldt, and Marc Heuse. *AFL++: Combining incremental steps of fuzzing research* in 14th USENIX Workshop on Offensive Technologies (WOOT 20). USENIX Association, Aug. 2020.

2020 Andrea Fioraldi, Daniele Cono D'Elia, and Leonardo Querzoni. *Fuzzing binaries for memory safety errors with QASan* in 2020 IEEE Secure Development Conference (SecDev), 2020.

Other

2019 Fioraldi Andrea, *Compare coverage for AFL++ QEMU*, https://andreafioraldi.github.io/articles/2019/07/20/aflpp-qemu-compcov.html

2019 Fioraldi Andrea, *Sanitized Emulation with QASan*, https://andreafioraldi.github.io/articles/2019/12/20/sanitized-emulation-with-qasan.html

Technical Skills

Programming Languages

I am very proficient with C, C++, Python, ASM x86 and I am familiar with Javascript, Java, Scala, C#.

Operating Systems

I am skilled in writing code for POSIX systems and I am not bad with MS Windows (userspace development). I know the internals of the Linux operating system and I am familiar with the kernel codebase.

Security Tools

I know very well how to use IDA Pro, GDB, Frida and Intel PIN and I also know how to use and the internals of American Fuzzy Lop, QEMU TCG and angr. I have a limited past experience with radare2.

Past Works

2020 Student researcher in the S3 Lab of EURECOM under the supervision of Prof. D. Balzarotti.

Voluntary

2018-2020 Binary exploitation teacher at CyberChallenge.IT in Rome

2020 Google Summer of Code admin and mentor for the AFL++ organization

Hobbies and Passions

Play the trumpet • Homebrewing • Trekking • Mountain bike

Last updated: October 19, 2020 • Typeset in XƎTEX

https://raw.githubusercontent.com/andreafioraldi/CurriculumVitae/master/cv.pdf

Italian legal note: Autorizzo il trattamento dei miei dati personali presenti nel cv ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” e del GDPR (Regolamento UE 2016/679)