
Giulio De Pasquale

COMPUTER SECURITY ENGINEER

☎ (+39) 348 340 2033 | ✉ me@giugl.io | 🏠 peperunas.github.io | 📠 peperunas | 📺 giuliodepasquale | 🐦 peperunas

Education

Ph.D Candidate in Computer Security

London, United Kingdom

KING'S COLLEGE LONDON, DEPARTMENT OF INFORMATICS

November 2018 - PRESENT

Post-graduate research programme covering a wide spectrum of Computer Security topics, focusing mainly on **program analysis**. Other research interests include binary obfuscation/deobfuscation methodologies, malware analysis and vulnerability identification and exploitation.

Advised by Professor Lorenzo Cavallaro.

B.Sc Degree in Engineering of Computing Systems

Milan, Italy

POLITECNICO DI MILANO

September 2011 - September 2017

Degree that covers all the fundamental topics in the IT area, such as Algorithms, Operating Systems, Databases and Computer Architectures, combined to major Engineering subjects including Physics, Math and Algebra.

Experience

Research Intern - NExT Special Projects

Redmond, Washington, USA

MICROSOFT RESEARCH

June 2019 - September 2019

Researched **malware analysis** techniques on **ELF core** files as part of *Microsoft Project Freta*. The project has been developed in **Rust**.

Advised by Mike Walker.

- **Webpage:** <https://aka.ms/freta>

Visiting Graduate Researcher - SecLab

Santa Barbara, California, USA

UNIVERSITY OF CALIFORNIA, SANTA BARBARA

January 2018 - July 2018

Researched **binary deobfuscation** techniques and novel **fuzzing** methodologies targeting IOT devices.

Advised by Professors Christopher Kruegel and Giovanni Vigna.

Publications

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Los Angeles, California, USA

IN PROCEEDINGS OF THE ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC)

December 2016

ShieldFS is an innovative solution to fight **ransomware** attacks. It automatically creates detection models that distinguish ransomware from benign processes at runtime on the base of the filesystem activity. ShieldFS adapts these models to the filesystem usage habits observed on the protected system.

- **Authors:**

Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, **Giulio De Pasquale**, Alessandro Barengi, Stefano Zanero, Federico Maggi.

- **Webpage:** <http://shieldfs.necst.it>

Personal projects

Pasticciotto

Milan, Italy

PoLiCTF '17

June 2017

Pasticciotto is a polymorphic **Virtual Machine** which can be embedded in an application to protect proprietary code. It was developed for the **PoLiCTF '17** as a reverse engineering challenge. The project is open source and is written in **C++**.

- **Webpage:** <https://github.com/peperunas/pasticciotto>

Injectopi

Milan, Italy

POLITECNICO DI MILANO

February 2017 - May 2017

Injectopi is a set of tutorials that illustrates multiple **code injection** techniques in the Microsoft Windows environment. The project is open source and it is written in **C**.

- **Webpage:** <https://github.com/peperunas/injectopi>

AESTracer

Milan, Italy

POLITECNICO DI MILANO

October 2015 - January 2016

AESTracer is a **Microsoft Windows driver** which actively scans running processes for valid AES keyschedules. It has been included in a research project, ShieldFS, which was later published at ACSAC '16. The project was written in **C**.

Technical skills

Information Security	Data forensics, memory exploitation, network analysis
Operating Systems	Arch Linux, Gentoo, Debian, Ubuntu, Microsoft Windows, Mac OS X
Programming	C, Python, Rust, Bash, C++, Java, WINAPI
Reverse Engineering	IDA, Binary Ninja, Angr, Radare2
System Administration	Docker, iptables, Wireguard, OpenVPN, Restic, Systemd, Traefik

Language proficiency

2016	Test of English for International Communication (TOEIC) , 975/990	Milan, Italy
2011	Test of English as a Foreign Language (TOEFL) , 99/120	Lecce, Italy
2010	Cambridge English: Advanced (CAE) , B	Lecce, Italy

Research Labs

S2Lab

London, United Kingdom

KCL'S SYSTEMS SECURITY RESEARCH LAB

November 2018 - PRESENT

The Systems Security Research Lab (S2Lab) is part of the Cybersecurity group in the Department of Informatics at King's College London.

- **Webpage:** <https://s2lab.kcl.ac.uk/>

SecLab

Santa Barbara, California, USA

UCSB'S COMPUTER SECURITY RESEARCH LAB

January 2018 - July 2018

The Computer Security Group at UCSB works on tools and techniques for designing, building, and validating secure software systems.

- **Webpage:** <https://seclab.cs.ucsb.edu/>

NECSTLab

Milan, Italy

POLITECNICO DI MILANO'S NOVEL EMERGING COMPUTING SYSTEM TECHNOLOGIES LABORATORY

March 2014 - September 2017

The NECSTLab is a research laboratory of Politecnico di Milano focusing on a number of different research lines on advanced topics in computing systems.

- **Webpage:** <https://necst.it>

POuL Linux User Group

Milan, Italy

POLITECNICO OPEN UNIX LABS

March 2014 - PRESENT

I am an *honorary member* of POuL, a hackerspace and association of Politecnico di Milano students interested in Linux, hacking and FOSS.

- **Webpage:** <https://poul.org>

CTF Teams

mHACKeroni

Italy

ITALIAN CAPTURE THE FLAG (CTF) TEAM

May 2019 - PRESENT

mHACKeroni is a CTF team composed of 5 CTF Italian teams. We qualified to **DEFCON 2019 Finals** and placed 5th out of 16 finalists.

- **Webpage:** <https://mhackeroni.it/>

Phish 'n' Chips

London, United Kingdom

KING'S COLLEGE LONDON CAPTURE THE FLAG (CTF) TEAM

November 2018 - PRESENT

Founder of King's College London CTF team.

Shellphish

Santa Barbara, California, USA

UCSB'S CAPTURE THE FLAG (CTF) TEAM

January 2018 - July 2018

Helped to organize the **UCSB's iCTF 2018** competition.

- **Webpage:** <https://ictf.cs.ucsb.edu/>

Tower of Hanoi

Milan, Italy

POLITECNICO DI MILANO'S CAPTURE THE FLAG (CTF) TEAM

September 2014 - PRESENT

Helped to organize the **PoliCTF 2015** competition held during DIMVA 2015 in Milan.

- **Webpage:** <https://polictf.it>

Talks and Presentations

Advanced Course for Linux System Administration

Milan, Italy

POLITECNICO DI MILANO

March 2016

Introduced the main command line tools along with their usage. The course was mainly aimed at sysadmins and Linux enthusiasts.

- **Slides:** https://slides.poul.org/2016/corsi-linux-avanzati/Bash_e_Filtri.pdf

AESTracer - How to find AES keyschedules in kernel-space

Milan, Italy

NECSTLAB @ POLITECNICO DI MILANO

February 2016

Introduced Microsoft Windows driver development basics and how it is possible to hijack running processes in order to find valid AES keyschedules.

- **Slides:** <http://slides.com/giuliodepasquale/aestracer-aeshooker/>