Giulio **De Pasquale**

SECURITY ENGINEER

recruit@depasquale.giugl.io | pepe.runas.rocks | peperunas | giuliodepasquale | peperunas

Experience

Security Engineer
APPLE — *London, United Kingdom* — *October 2023 - PRESENT*

Security Engineer in Apple Information Security (AIS).
https://apple.com

Visiting PhD Student - SecLab
UNIVERSITY OF CALIFORNIA, SANTA BARBARA — *Santa Barbara, California, USA* — *June 2022 - October 2023*

Conducted research on the application of **AI planning** in post-exploitation scenarios. This involved automatically deriving system facts and creating action chains for privilege escalation. This work was a component of the DARPA HARDEN program.
https://seclab.cs.ucsb.edu | Advised by *Prof. Christopher Kruegel and Prof. Giovanni Vigna*

Research Internship
APPLE — *London, United Kingdom* — *May 2022 - June 2022*

Internship in the Applied Research team part of Apple Information Security (AIS).
https://apple.com | Advised by *Andre Protas*

Visiting PhD Student
UNIVERSITY COLLEGE OF LONDON — *London, United Kingdom* — *June 2021 - February 2024*

Joined UCL's ISec research group to collaborate on ongoing research projects. Coordinated an ongoing series of fortnightly **hands-on seminars** on information security while focusing on solving CTF challenges.
https://sec.cs.ucl.ac.uk

Research Intern
TWEAG I/O — *Remote* — *June 2021 - September 2021*

Worked on improving the robustness of the type system of **Nickel**, a declarative configuration language. The project is written in **Rust**.
https://github.com/tweag/nickel | Advised by *Dr. Yan Hamdaoui*

Research Intern - NExT Special Projects
MICROSOFT RESEARCH — *Redmond, Washington, USA* — *June 2019 - September 2019*

Researched **malware analysis** techniques to detect active threats in **ELF core** files as part of *Microsoft Project Freta*. The project has been developed in **Rust**.
https://aka.ms/freta | Advised by *Mike Walker*

Visiting Graduate Researcher - SecLab
UNIVERSITY OF CALIFORNIA, SANTA BARBARA — *Santa Barbara, California, USA* — *January 2018 - July 2018*

Researched **deobfuscation** techniques for software protected by VM obfuscation and **fuzzing** methodologies targeting IoT devices.
https://seclab.cs.ucsb.edu | Advised by *Prof. Christopher Kruegel and Prof. Giovanni Vigna*

Publications

ChainReactor: Automated Privilege Escalation Chain Discovery via AI Planning
Philadelphia, Pennsylvania, USA

33RD USENIX SECURITY SYMPOSIUM *(USENIX '24)* — *August 2024*

ChainReactor is a research project that leverages **AI planning** to discover exploitation chains for **privilege escalation** on Unix systems. The project models the problem as a sequence of actions to achieve privilege escalation from initial access to a target system. **Awarded the Distinguished Artifact Award.**

- **Authors:**
  Giulio De Pasquale, *Ilya Grishchenko, Riccardo Iesari, Gabriel Pizarro, Lorenzo Cavallaro, Christopher Kruegel and Giovanni Vigna.*

ROPfuscator: Robust Obfuscation with ROP

San Francisco, California, USA

17th IEEE Workshop on Offensive Technologies *(WOOT '23)* *May 2023*

Based on Return-Oriented Programming (ROP), ROPFuscator is a compiler-driven software **obfuscation pass**, developed to protect intellectual property in software from sophisticated man-at-the-end (MATE) attacks and reverse engineering attempts.

- **Authors:**
  Giulio De Pasquale, *Fukutomo Nakanishi, Daniele Ferla, Lorenzo Cavallaro.*

DIANE: Identifying Fuzzing Triggers in Apps to Generate Under-constrained Inputs for IoT Devices

Online

42nd IEEE Symposium on Security and Privacy *(S&P)* *May 2021*

DIANE is a tool that combines static and dynamic analysis to find **fuzzing triggers** and uses them to fuzz IoT devices automatically.

- **Authors:**
  Nilo Redini, Andrea Continella, Dipanjan Das, ***Giulio De Pasquale****, Noah Spahn, Aravind Machiry, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna.*

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Los Angeles, California, USA

32nd Annual Computer Security Applications Conference *(ACSAC)* & Black Hat '17 *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 Barenghi, Stefano Zanero, Federico Maggi.*

Education

Ph.D Degree in Computer Security

London, United Kingdom

King's College London, Department of Informatics *November 2018 - February 2024*

Post-graduate research program 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.

https://s2lab.kcl.ac.uk | Advised by *Prof. 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 with major Engineering subjects including Physics, Math, and Algebra.

Technical skills

Operating Systems	Gentoo, NixOS, Arch Linux, Debian, Ubuntu, Microsoft Windows, MacOS
Programming	Python, Rust, Golang, Nix, C, Souffle, PDDL, TypeScript, Bash, C++, Java
Interests	Reverse engineering, program analysis, system administration, declarative, low-level and systems' programming

Personal projects

Rustico

Rustico is a **Rust** cryptocurrency trading bot. It is features a frontend developed with **Svelte and TailwindCSS** and it is extendable with user-programmed trading strategies.

Pasticciotto

https://github.com/peperunas/pasticciotto

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 it is written in **C++**.

Injectopi https://github.com/peperunas/injectopi

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**.

AESTracer

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**.

Conferences contributions

Program Committee *USENIX* 2019, *WOOT* 2023, *ESORICS* 2023
Artifact Evaluation Committee *USENIX* 2021/2022/2023/2024, *NDSS* 2023, *WOOT* 2023

CTF Teams

mHACKeroni *Italy*
Italian Capture the Flag (CTF) Team *May 2019 - PRESENT*

mHACKeroni is composed by five CTF Italian teams. We qualified and placed 5th to **DEFCON 2019 Finals**.

- Involved in the organization of the **mHACKeCTF '20** competition.
  https://mhackeroni.it

Phish 'n' Chips *London, United Kingdom*
King's College London Capture the Flag (CTF) Team *November 2018 - PRESENT*

- Founder of the team.
  https://phishnchips.co.uk

Shellphish *Santa Barbara, California, USA*
UCSB's Capture the Flag (CTF) Team *January 2018 - PRESENT*

- Involved in the organization of the **UCSB's iCTF 2018** competition.
  https://ictf.cs.ucsb.edu/

Tower of Hanoi *Milan, Italy*
Politecnico di Milano's Capture the Flag (CTF) Team *September 2014 - PRESENT*

- Involved in the organization of the **PoliCTF 2015** competition held during DIMVA 2015 in Milan.
  https://polictf.it

Volunteering

Residence Welfare Lead *London, United Kingdom*
King's Residences *January 2021 - June 2022*

Residence Welfare Leads are recruited to help residents in King's residences. Welfare Leads are specially trained to live in the Halls and provide an out-of-hours wellbeing support service to our residents, including first aid, mental health and crisis prevention.

Dog Volunteer *Santa Barbara, California, USA*
Santa Barbara Humane *March 2023 - October 2023*

As a Dog Volunteer, daily care was provided for shelter dogs, including exercise, basic training, and socialization. The role involved maintaining the cleanliness of the housing environment, reporting any concerns, and assisting in the adoption process. Operational tasks such as feeding and spot cleaning were also performed. The volunteers are trained in safe animal handling, positive reinforcement training, and reporting changes in animal behavior or health.