Fabio Pagani

Affiliation

Vulnerability Research Lead, Binarly

Contact Information

pagani@ucsb.edu
https://pagabuc.me
@pagabuc
FabioPagani

Bio

I am a Vulnerability Research Lead at Binarly, where I work at the intersection of static and dynamic analysis techniques to help secure the UEFI ecosystem.

Previously, I was a postdoctoral researcher working with Giovanni Vigna and Christopher Kruegel in the SecLab at UC Santa Barbara. My current research interests focus on different aspects of systems security: automated vulnerability discovery, human-assisted cyber reasoning systems, and malware analysis are all topics that spark my curiosity.

I earned a Ph.D at EURECOM, where I was advised by Davide Balzarotti. Among other things, we investigated how non-atomic acquisitions impact the consistency of memory dumps, how to discover and to assess the quality of memory forensics heuristics, and how to automatically generate profiles for memory forensics.

When I am away from keyboard, I enjoy hiking, rock climbing, surfing, and playing chess.

Experience

Vulnerability Research Lead *Jun 2024-Present*
Binarly

Principal Research Scientist *Mar 2023-Jun 2024*
Binarly

Postdoctoral Researcher *Jan 2020-Mar 2023*
University of California, Santa Barbara, US

Doctor in Philosophy (PhD) *Jan 2016-Sept 2019*
Eurecom, France
Thesis: Advances in Memory Forensics

Education

MSc in Computer Science *Feb 2013-Oct 2015*
Universitá degli Studi di Milano, Italy
Thesis: Defeating Return Oriented Programming Attacks Using Program Analysis Techniques
Graduated with a final grade of 110/110 cum laude

Internship *Feb 2015-May 2015*
Eurecom, France

Erasmus *Jan 2014-Jun 2014*
Uppsala University, Sweden

BSc in Computer Science *Sep 2009-Feb 2013*
Universitá degli Studi di Milano, Italy
Thesis: When Hardware Meets Software: A Bulletproof Solution to Forensic Memory Acquisition
Graduated with a final grade of 107/110

Talks

[5] **Fabio Pagani**, Alex Matrosov, Yegor Vasilenko, Sam Thomas, Anton Ivanov. PKfail: Supply-Chain Failures in Secure Boot Key Management. LABScon 2024

[4] **Fabio Pagani**, Alex Matrosov, Alex Ermolov, Yegor Vasilenko, Sam Thomas, Anton Ivanov. LogoFAIL: Security Implications of Image Parsing During System Boot. BlackHat EU 2023

[3] Victor Duta, Fabian Freyer, **Fabio Pagani**, Marius Muench, Cristiano Giuffrida. Unwinding the Stack for Fun and Profit. Black Hat EU 2022

[2] Nicola Ruaro, **Fabio Pagani**, Stefano Ortolani, Giovanni Vigna. Symbexcel: Bringing the Power of Symbolic Execution to the Fight Against Malicious Excel 4 Macros. Black Hat USA 2021

[1] **Fabio Pagani**. Memory Smearing: Myth Or Reality?. SANS DFIR Europe Summit 2019

Publications

[14] Victor Duta, Fabian Freyer, **Fabio Pagani**, Marius Muench, Cristiano Giuffrida. Let Me Unwind That For You: Exceptions to Backward-Edge Protection. In Proceedings of the Network and Distributed Systems Security Symposium (NDSS 2023)

[13] Erik Trickel, **Fabio Pagani**, Chang Zhu, Lukas Dresel, Giovanni Vigna, Christopher Kruegel, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, Adam Doupe. Toss a Fault to Your Witcher: Applying Grey-box Coverage-Guided Mutational Fuzzing to Detect SQL and Command Injection Vulnerabilities. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (IEEE S&P 2023)

[12] Kevin Burk, **Fabio Pagani**, Christopher Kruegel, Giovanni Vigna. Decomperson: How Humans Decompile and What We Can Learn From It. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)

[11] Nicola Ruaro, **Fabio Pagani**, Stefano Ortolani, Christopher Kruegel, Giovanni Vigna. Symbexcel: Automated Analysis and Understanding of Malicious Excel 4.0 Macros. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (IEEE S&P 2022)

[10] Fabio Gritti, **Fabio Pagani**, Ilya Grishchenko, Lukas Dresel, Nilo Redini, Christopher Kruegel, Giovanni Vigna. HEAPSTER: Analyzing the Security of Dynamic Allocators for Monolithic Firmware Images. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (IEEE S&P 2022)

[9] **Fabio Pagani**, Davide Balzarotti. AutoProfile: Towards Automated Profile Generation For Memory Analysis. ACM Transactions on Privacy and Security (TOPS) 25, no. 1 (2022)

[8] Robert McLaughlin, **Fabio Pagani**, Noah Spahn, Christopher Kruegel, Giovanni Vigna. Regulator: Dynamic Analysis To Detect ReDoS. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)

[7] Fabio Gritti, Lorenzo Fontana, Eric Gustafson, **Fabio Pagani**, Andrea Continella, Christopher Kruegel, Giovanni Vigna. SYMBION: Interleaving Symbolic With Concrete Execution. In Proceedings of the IEEE Conference on Communications and Network Security (CNS) 2020

[6] **Fabio Pagani**, Davide Balzarotti. Back to the Whiteboard: a Principled Approach for the Assessment and Design of Memory Forensic Techniques. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19) 2019

[5] **Fabio Pagani**, Oleksii Fedorov, Davide Balzarotti. Introducing the Temporal Dimension to Memory Forensics. ACM Transactions on Privacy and Security (TOPS) 22, no. 2 (2019)

[4] **Fabio Pagani**, Matteo Dell'Amico, Davide Balzarotti. Beyond Precision and Recall: Understanding Uses (and Misuses) of Similarity Hashes in Binary Analysis. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY) 2018

[3] Marius Muench, **Fabio Pagani**, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna, Davide Balzarotti. Taming Transactions: Towards Hardware-Assisted Control Flow Integrity Using Transactional Memory. In International Symposium on Research in Attacks, Intrusions, and Defenses (RAID) 2016

[2] **Fabio Pagani**, Matteo De Astis, Mariano Graziano, Andrea Lanzi, Davide Balzarotti. Measuring the Role of Greylisting and Nolisting in Fighting Spam. In Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2016

[1] Alessandro Reina, Aristide Fattori, **Fabio Pagani**, Lorenzo Cavallaro, Danilo Bruschi. When Hardware Meets Software: a Bulletproof Solution to Forensic Memory Acquisition. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC) 2012

Awards

[3] Distinguished Reviewer Award - DIMVA 2021

[2] Volatility Plugin Contest 2019, 5th place

[1] Black Hat Europe 2016 Student Scholarship

Service

IEEE Workshop on Offensive Technologies (WOOT) 2024

USENIX Security 2024

IEEE Symposium on Security and Privacy (S&P) 2023

Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2023

IEEE Workshop on Offensive Technologies (WOOT) 2023

Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2022

Digital Forensics Research Workshop (DFRWS) USA 2022

IEEE Workshop on Offensive Technologies (WOOT) 2022

Workshop on Binary Analysis Research (BAR) 2022

Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2021

Computers & Security (COSE)

Teaching Experience

Lecture on Memory Forensics (Cybercrime and Computer Forensics) *Apr. 2019*
Eurecom, France

Lecture on Python Optimization and Integration (Software Development) *Dec. 2018*
Eurecom, France

Lecture on Memory Forensics (Cybercrime and Computer Forensics) *May 2018*
Eurecom, France

Lecture on Python Optimization and Integration (Software Development) *Dec. 2017*
Eurecom, France

Lecture on Python Optimization and Integration (Software Development) *Dec. 2016*
Eurecom, France

Computer Programming - Teaching Assistant *Sept. 2014 - Feb. 2015*
Universitá degli Studi di Milano, Italy

Hacking Competitions

I am part of Shellphish, and I helped with the organization of iCTF 2021 and Decompetition V1 and V2.

I am also a core member of the NOPS team. As a team, we qualified twice for the CSAW Europe Finals (with a 2nd place in 2017) and we **won** hxp CTF 2018.