UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Activities and Publications Report

PhD Student: Carmine Cesarano

Student DR number: DR996627

PhD Cycle: XXXVIII
PhD Chairman: Prof. Stefano Russo

PhD program student's start date: 01/11/2022
PhD program student's end date: 31/10/2025

Supervisor: Prof. Roberto Natella

E-mail: roberto.natella@unina.it

Co-supervisor:

e-mail:

PhD scholarship funding entity:
Università Federico II

General information

Dr. Carmine Cesarano received in year 2022 the Master Science degree in Computer Engineering from the University of Napoli Federico II. Within the PhD program in Information Technology and Electrical Engineering, he attended a curriculum in Computer Engineering. He received a grant from Università Federico II.

Study activities

Attended Courses

Year	Course Title	Type	Credits	Lecturer	Organizer(s)
1st	IoT Data Analysis	Ad hoc course	4	Prof. Raffaele Della Corte	ITEE PhD Program
1st	Virtualization Technologies and their applications	Ad hoc course	5	Prof. Luigi De Simone	ITEE PhD Program
1st	Statistical Data Analysis for Science and Engineering Research	Ad hoc course	4	Prof. Roberto Pietrantuono	ITEE PhD Program
2nd	Percorso per il rafforzamento delle competenze sulla progettazione europea	External Course	3,4	Dr. Tommaso Foglia	UNINA
2nd	Strategic Orientation for STEM Research & Writing	Ad hoc course	5	Arianna D’Auria	ITEE PhD Program
2nd	Using Deep Learning Properly	Ad hoc course	4	Dr. Andrea Apicella	ITEE PhD Program
3rd	Innovation and Entrepreneurship	Ad hoc course	3	Prof. Pierluigi Rippa	ITEE PhD Program
3rd	AI Code Generation: Foundations, Evaluation, and Security	Ad hoc course	3	Dr. Pietro Liguori	ITEE PhD Program

Attended PhD Schools

Year	School title	Location	Credits	Dates	Organizer(s)
-	-	-	-	-	-

Attended Seminars

Year	Seminar Title	Credits	Lecturer	Lecturer affiliation	Organizer(s)
1st	From Cyber Situational Awareness to Adaptive Cyber Defense: Leveling the Cyber Playing Field	0.4	Prof. Massimiliano Albanese	George Mason University	ITEE
1st	Industry 4.0 Fundamentals in Bosh Applications	2	Prof. Mariagrazia Dotoli	Politecnico di Bari	National Ph.D. Program in Autonomous Systems
1nd	Open-source software e sicurezza della software supply chain	0.2	Antonino Sabetta	SAP	ITEE
1nd	Traffic Engineering with Segment Routing: optimally dealing with most popular use-cases	0.2	Prof. Pascal Merindol	University Catholique of Louvain	ITEE
1nd	Exploring Advanced Aerials Robotics: A Journey into Cutting-Edge Projects and Neural Control	0.2	Dr. Eugenio Cuniato	ETH Zurich	ITEE
1nd	Models of human motor coordinator – a critical assessment and some open problems	0.2	Dr. John Hogan	University of Bristol	Scuola Superiore Meridionale
1nd	BGP and Hot-Potato Routing: optimal convergence in the case of IGP events	0.2	Prof. Pascal Merindol	University Catholique of Louvain	ITEE
1nd	Ricerca e formazione nella società della transizione digitale	1	Prof. Nicola Mazzocca	University of Naples Federico II	Consorzio CINI
2nd	Energy-Efficient Data Science	0.2	Dr. Carlos Ordonez	University of Houston	ITEE
2nd	Simplifying Supply Chain Security at GitHub	0.2	Eng. Fredrik Skogman	GitHub	KTH Stockholm University
2nd	RepairLLaMA: Efficient Representation	0.2	Dr. André Silva	KTH Stockholm University	KTH Stockholm University
2nd	4th generation HW-design	0.2	Wolfang	University of	European Dependable

			Ecker	Munich	Computing Conference 2024
2nd	Privacy-friendly P2P energy trading market	0.2	Dr. Mustafa A. Mustafa	Un iversity of Manchester	European Dependable Computing Conference 2024
2nd	Keynote: Safety programmable logic controllers	0.2	Eng. Geert Bogaerts	Equans BeLux	European Dependable Computing Conference 2024
2nd	IEEE Authorship and Open Access Symposium: Tips and Best Practices to Get Published from IEEE Editors	0.4	Rachel Berrington	IEEE	ITEE
2nd	Detecting Vulnerabilities in Blockchain Layer 2 Software Clients	0.2	Dr. Karolina Gorna	Télécom Paris	KTH Stockholm University
2nd	Keynote: Cryptographic and Computer Security: A View From the Year 2100	0.2	Prof. Dan Boneh	Stanford University	Computer and Communication Systems Conference 2024
2nd	Keynote: Starving off the IoT Armageddon	0.2	Prof. Gene Tsudik	University of California	Computer and Communication Systems Conference 2024
2nd	Keynote: Insane in the AI Supply Chain: Attacks, defenses and open questions	0.2	Eng. Eon Wickens	HiddenLayer	Computer and Communication Systems Conference 2024
3nd	Safety Assessment of Autonomous Vehicles: Approaches and Challenges	0.2	Prof. Peter Popov	City University of London	ITEE
3nd	On the Notion of binary equivalence in software supply chain security	0.2	Prof. Jens Dietrich	Victoria University of Wellington	ITEE
3nd	On the security of semantic watermarking to detect AI-generated content	0.2	Dr. Erwin Quiring	Ruhr University Bochum	ITEE
3nd	Phd Survival Strategies	0.3	Prof. Gabriele Bavota	Università della Svizzera Italiana	ITEE

Research activities

Carmine Cesarano conducted his research within the *Dependable and Secure Software Engineering and Real-Time Systems* group, focusing on attack surface reduction in complex, layered infrastructures that integrate orchestration, virtualization, inter-process communication (IPC), and open-source supply chains. His work advances automated, fine-grained, and resilient techniques to minimize the exposed interfaces through which modern systems can be attacked, contributing to the state of the art in orchestration security, binary fuzzing, hypervisor analysis, and supply chain protection. His research addresses how adversaries exploit the heterogeneity of contemporary software stacks, through over-privileged orchestration APIs, opaque IPC channels in proprietary binaries, and untrusted open-source dependencies. To counter these threats, he developed complementary approaches that harden each class of interface: (1) enforcing least privilege and runtime policy derivation in orchestrator APIs; (2) enabling emulation-based fuzzing to expose hidden IPC vulnerabilities; and (3) monitoring and constraining open-source components through package-level runtime enforcement.

Tutoring and supplementary teaching activities

The candidate has performed supplementary teaching activities (“didattica integrativa”) for the course “Software Security” held by prof. Roberto Natella, within the Msc Degree in Computer Engineering at Federico II University, for the academic year 2022-2023.

Credits summary

PhD Year	Courses	Seminars	Research	Tutoring / Supplementary Teaching
1st	13	4.4	40.5	1.5
2nd	12.4	2.4	45.2	0
3rd	6	0.9	53.7	0

Research periods in institutions abroad and/or in companies

PhD Year	Institution / Company	Hosting tutor	Period	Activities
1st	KTH Royal Institute of Technology in Stockholm (Sweden)	Prof. Martin Monperrus	01/03/2024 - 31/08/2024	Research on open-source software supply chain security. Joint scientific paper preparation “GoSurf: Identifying Software Supply Chain Attack Vectors in Go”

PhD Thesis

In the PhD Thesis, Carmine Cesarano addresses the scientific problem of how to automate attack surface reduction across multiple abstraction layers of modern software systems. He proposes novel methods that combine static and dynamic analysis to achieve fine-grained, workload-specific, and evasion-resilient security. The thesis introduces five original techniques, including KubeFence, FuzzBox, IRIS, GoSurf, and GoLeash, each targeting a distinct attack surface (orchestration, IPC, hypervisor, and software supply chain). Together, these contributions provide new foundations and practical tools for securing open, heterogeneous, and deeply layered infrastructures.

Research products

Research results appear in 2 papers published in international journals and 9 papers published in national journals.

List of scientific publications

International journal papers

C. Cesarano, A. Foggia, G. Roscigno, L. Andreani and R. Natella
GENIO: Synergizing Edge Computing with Optical Network Infrastructures
IEEE Communications Magazine, vol. 63, no. 7, pp. 154-160, July 2025, doi: 10.1109/MCOM.002.2400382.

Cesarano, C., Natella, R.
FuzzBox: Blending Fuzzing into Emulation for Binary-Only Embedded Targets
Springer Cybersecurity Journal
Under publication, DOI: 10.1186/s42400-025-00474-2.

International conference papers

C. Cesarano, D. Cotroneo and L. De Simone
Towards Assessing Isolation Properties in Partitioning Hypervisors
IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)
Charlotte, NC, USA, 2022, pp. 193-200, doi: 10.1109/ISSREW55968.2022.00067.

C. Cesarano, M. Cinque, D. Cotroneo, L. De Simone and G. Farina
IRIS: a Record and Replay Framework to Enable Hardware-assisted Virtualization Fuzzing
53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)
Porto, Portugal, 2023, pp. 389-401, doi: 10.1109/DSN58367.2023.00045.

C. Cesarano
Security Assessment and Hardening of Fog Computing Systems
IEEE 34th International Symposium on Software Reliability Engineering Workshops (ISSREW)
Florence, Italy, 2023, pp. 22-25, doi: 10.1109/ISSREW60843.2023.00037.

C. Cesarano, V. Andersson, R. Natella, and M. Monperrus
GoSurf: Identifying Software Supply Chain Attack Vectors in Go
Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED '24).
New York, NY, USA, 33–42. https://doi.org/10.1145/3689944.3696166

C. Cesarano and R. Natella
Securing an Application Layer Gateway: An Industrial Case Study

2024 19th European Dependable Computing Conference (EDCC)
Leuven, Belgium, 2024, pp. 75-80, doi: 10.1109/EDCC61798.2024.00025.

C. Cesarano and R. Natella
KubeFence: Security Hardening of the Kubernetes Attack Surface
55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)
Naples, Italy, 2025, pp. 497-510, doi: 10.1109/DSN64029.2025.00054.

C. Cesarano, A. Foggia, G. Roscigno, L. Andreani and R. Natella
Security-by-Design at the Telco Edge with OSS: Challenges and Lessons Learned
55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)
Naples, Italy, 2025, pp. 49-55, doi: 10.1109/DSN-S65789.2025.00041.

Cesarano C., Natella R.
KubeFence: Security Hardening of the Kubernetes Attack Surface
55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)
Naples, Italy, 23-26 June 2025, IEEE, DOI: 10.1109/DSN64029.2025.00054.

Cesarano, C., Foggia, A., Roscigno, G., Andreani, L., Natella, R
Security-by-Design at the Telco Edge with OSS: Challenges and Lessons Learned
55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S)
Naples, Italy, 23-26 June 2025, IEEE, DOI: 10.1109/DSN-S65789.2025.00041

Patents and/or spin offs

-

Awards and Prizes

-

Date 27/10/2025

Carmine Cesarano

PhD student signature ____________________

Supervisor signature ____________________