UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

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

Activities and Publications Report

PhD Student: Francesco Caputo

Student DR number: DR996113

PhD Cycle: XXXVII
PhD Cycle Chairman: Prof. Stefano Russo

PhD program student's start date: 01/01/2022
PhD program student's end date: 31/12/2024

Supervisor: Prof. Pasquale Arpaia

e-mail: pasquale.arpaia@unina.it

Co-supervisor: Nicola Moccaldi

e-mail: Nicola.moccaldi@unina.it

PhD scholarship funding entity:
PON "Ricerca ed innovazione" 2014-2020, Azione IV.5 – "Dottorati di ricercar su tematiche Green"

General information

Francesco Caputo received in year 2021 the Master Science degree in Electronic Engineering from the University of Napoli Federico II. He attended a curriculum in Cybersecurity for Smart Industries within the PhD program in Information Technology and Electrical Engineering. He received a grant from "PON Ricerca ed innovazione 2014-2020".

Study activities

Attended Courses

Year	Course Title	Type	Credits	Lecturer	Organization
1st	Statistical data analysis for science and engineering research	Ad hoc course	4	Roberto Pietrantuono	ITEE
2nd	Laboratorio di programmazione	MSc course	9	Luigi De Simone	University of Napoli "Federico II"
3rd	Machine Learning for Science and Engineering Research	Ad hoc course	5	Proff. Anna Corazza, Francesco Isgrò, Roberto Prevete, Carlo Sansone, Dott. Giovanni Pezzulo	ITEE
4th	Metrology and machine learning for brain computer interfaces	Ad hoc course	3	Pasquale Arpaia	ITEE
5th	Sustainable Ship For The Energy Transition Of Maritime Transport	Ad hoc course	4	Tommaso Coppola	ITEE
6th	Using Deep Learning properly		4	Andrea Apicella	ITEE
7th	The Deep Edge	External Course	1,5	Davide Ruggiero	STMicroelectronics, Arzano
8th	Big Data Architecture and Analytics		5	Giancarlo Sperlì	ITEE

Attended PhD Schools

Year	School title	Location	Credits	Dates	Organization

Attended Seminars

Year	Seminar Title	Credits	Lecturer	Lecturer affiliation	Organization
1st	An Introduction to Deep Learning for Natural Language Processing	0,2	Marco Valentino	University of Napoli Federico II	ITEE

2nd	Using Delays For Control (Part 1)	0,2	Dariusz Horla	University of Napoli Federico II	ITEE
3rd	On using simple optimization tecniques for tuning of UAVs	0,4	Prof. Emilia Fridman	University of Napoli Federico II	ITEE
4th	Probing and infusing biomedical knowledge for pre-trained language models	0,4	Dr. ZAIQIAO MENG	University of Napoli Federico II	ITEE
5th	Variable IO Latencies in real life	0,4	Luca Porzio, Roberto Izzi, Dionisio Minopoli	University of Napoli Federico II	ITEE
6th	Come scrivere un CV	0,4	Prof. Pasquale Arpaia	University of Napoli Federico II	CIRMIS
7th	IEEE Xplore Webinar: Search Strategies to Maximize Your Research Experience	0,2	Rachel Berrington	IEEE	IEEE
8th	IEEE Authorship and Open Access Symposium: Tips and best practies to get published from IEEE Editors	0,3	Rachel Berrington	IEEE	IEEE
9th	Connecting the dots: Investigating an APT campaign using Splunk	0,4	Dr. Antonio Forzieri	University of Napoli Federico II	University of Napoli Federico II
10th	Cybercrime and Information Warfare: National and International Actors	0,4	Dr. Pierluigi Paganini	University of Napoli Federico II	University of Napoli Federico II
11th	Digitalizzazione dei processi di selezione	0,4	Adecco Group	Adecco	Adecco Group
12th	Accelerate Battery Development with Unified Design, Modeling and Simulation	0,2	Stephen Phillips	IEEE	IEEE
13th	AI Standards: Ethical Considerations And Best Practices When Implementing AI in your organization	0,2	Stephen Phillips	IEEE	IEEE
14th	Seminar: Game theory for information engineering	0,6	Prof. Leonardo Badia	University of Napoli Federico II	University of Napoli Federico II

15th	Data mining the output of quantum simulators from critical behavior to algorithmic complexity	0,4	Stephen Phillips	IEEE	IEEE
16th	Industry 4.0 Fundamentals in Bosch Applications	2	Eng. Martino Bruni	Polytechnic of Bari	ITEE
17th	The new Artificial Intelligence and its applications	0,2	Prof. Roberto Prevete	University of Napoli Federico II	University of Napoli Federico II
18th	Risk-Based Methodology For Deriving Scenarios For Testing Artificial Intelligence Systems	0,2	Stephen Phillips	IEEE	IEEE
19th	Human Vs. "Digital Driver" – Compliance And Homologation Challenges In The Automotive Industry	0,4	Stephen Phillips	IEEE	IEEE
20th	MetroXRAINE 2024	5	Pasquale Arpaia	CIRMIS	CIRMIS

Research activities *(research subjects and contributions – about 200 words)*

Francesco Caputo explored the use of machine learning in embedded environments as an alternative to massive data center usage. This new frontier of research allows to reduce the energy costs by moving artificial intelligence on the device compared to cloud solutions that have very high energy impacts.

The use of embedded machine learning solutions poses unique challenges both from the point of view of energy efficiency and usage, given the limited resources of devices, as well as from the point of view of security.

The research has led to first analyze what can be the vulnerabilities related to embedded devices from a strictly metrological point of view, such as side-channel and fault attack, applying different statistical techniques such as scatter and machine learning, To retrieve sensitive information from the device (e.g. encryption keys).

The research has continued in the analysis of the techniques for evaluating the performance of embedded devices, both from the energy point of view and from the point of view of the efficient use of available resources, and in the implementation of advanced evaluation techniques with full metrological rigour, providing added value by introducing an estimation of uncertainty and precision linked to measurements.

The work has been presented to several international conferences and to an international organization MLCommons which aims at standardizing a method of evaluating the performance cited.

Future development involves the use of embedded AI as a countermeasure to the cyber-physical attacks analysed so far, and the development of techniques for optimizing machine learning models so that integration can be made more efficient, Allowing the use of less and less centralized processing systems.

Tutoring and supplementary teaching activities

None

Credits summary *(Sum up all earned credits)*

PhD Year	Courses	Seminars	Research	Tutoring / Supplementary Teaching
1st	25,0	5,1	30,0	0,0
2nd	10,5	6,8	43,0	0,0
3rd	0,0	5,0	55,0	0,0

Research periods in institutions abroad and/or in companies

PhD Year	Institution / Company	Hosting tutor	Period	Activities
1st	STMicroelectronics, Marcianise, Italy	Luigi Capobianco, Quality assurance engineer	01/01/2022 31/12/2022	Study on Side-Channel Attacks with and without use of machine learning Study on Differential Power Analysis Study on Machine Learning Study on Secure Elements communication protocols Preparation of paper Side Channel Attacks with Machine Learning Laboratory activity on acquisition of power traces for Side Channel Attacks Laboratory activity on Power Traces acquisition from embedded devices Study on Python programming language Preparation of paper Side-Channel Attacks with Neural Network Laboratory activity on Power Traces acquisition from embedded devices
1st	CSLab, STMicroelectronics, Rousset, Italy (Remote)	Ettore Toscano, Site manager	12/02/2024 12/08/2024	Study on fault attacks on silicon devices with laser Laboratory activity on preparation of sample Laboratory activity on dataset construction for fault attacks Study on embedded code analysis for fault protection

PhD Thesis *(abstract 100-500 words)*

In the PhD Thesis, Francesco Caputo addresses the problem of using embedded solutions for the use of artificial intelligence models, increasingly present but less preferred than cloud solutions, due to limited resources available, Exploring energy performance, calculation and safety evaluation techniques. In particular, it will address the problem of performance evaluation regarding the integration of neural networks in embedded environments, as a tool to optimize the integration itself, and in full metrological rigor. Finally, it will address the problem of cyber-physical attacks and the application of statistical techniques to assess the efficiency of the attack. These methods can be used as a tool to establish, by means of a specific metric, the ability of a device to resist certain attacks.

Research products

The results of the research were presented in 3 papers published in international journals, 2 papers at international conferences and 1 demo at an international conference.

List of scientific publications *(list papers in the following format – remove categories with no publications)*

International journal papers

P.Arpaia, F.Caputo, A.Cioffi, A.Esposito, F.Isgrò,
Uncertainty Analysis in Cryptographic Key Recovery for Machine Learning-Based Power Measurements Attacks,
IEEE Transactions on Instrumentation and Measurement,
vol. 72, 2023, DOI: 1006108.

P.Arpaia, F.Caputo, A.Cioffi, A.Esposito,
The role of metrology in the cyber-security of embedded devices,
Acta IMEKO,
vol. 12, Number 2, 1 – 6

International conference papers

P.Arpaia, L.Capobianco, F.Caputo, A.Cioffi, A.Esposito, F. Isgrò, N. Moccaldi, D.Pau, D. Siorpaes, E. Toscano
Accurate Energy Measurements for TinyML Workloads,
TinyML Summit 2024

P.Arpaia, L.Capobianco, F.Caputo, A.Cioffi, A.Esposito, F. Isgrò, N. Moccaldi, D.Pau, D. Siorpaes, E. Toscano
Accurate Energy Measurements for TinyML Workloads,
IEEE MetroXRAINE International conference, 2024

National journal papers

None

National conference papers

None

Patents and/or spin offs

None

Awards and Prizes

None

Date 14/12/2024

PhD student signature _____

Supervisor signature _____