PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

PhD Student: Francesco Caputo

Cycle: XXXVII

Training and Research Activities Report

Academic year: 2022-2023 - PhD Year: Second

student signature

Tutor: prof. Pasquale Arpaia

tutor signature

Co-Tutor:

Date: December 12, 2023

1. Information:

- **PhD student: Francesco Caputo** **PhD Cycle: 37**
- **DR number: DR996113**
- **Date of birth: 26/12/1992**
- **Master Science degree: Electronic Engineering** **University: University of Napoli "Federico II"**
- **Scholarship type: MUR PON**
- **Tutor: Pasquale Arpaia**
- **Co-tutor:**

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Using Deep Learning properly	Course	10	4	10-12-17-19-24/01/2023	Andrea Apicella	Y
The Deep Edge	Course	14	1,5	01-02/02/2023	STMicroelectronics	Y
Big Data Architecture and Analytics	Course		5	26-29/06 06-07-10-12-14-19-20/07/2023	Giancarlo Sperlì	Y
Industry 4.0 Fundamentals in Bosch Applications	Seminar		2	23-26/01/2023	Prof. Ing. Mariagrazia Dotoli, Ph.D.	Y
The new Artificial Intelligence and its applications	Seminar	1	0,2	28/02/2023	Roberto Prevete	Y
Risk-Based Methodology For Deriving Scenarios For Testing Artificial Intelligence Systems	Seminar	1	0,2	26/04/2023	IEEE Seminars	N
Human Vs. "Digital Driver" - Compliance And Homologation Challenges In The Automotive Industry	Seminar	2	0,4	16/06/2023	IEEE Seminars	N
2023 IEEE International Conference On Metrology for eXtended Reality,	Seminar		4	25-27/10/2023	Pasquale Arpaia	Y

Artificial Intelligence and Neural Engineering Milan						

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	**5,5**	**2,2**	**8,0**	**0,0**	**15,7**
Bimonth 2	**0,0**	**0,2**	**8,0**	**0,0**	**8,2**
Bimonth 3	**0,0**	**0,4**	**8,0**	**0,0**	**8,4**
Bimonth 4	**5,0**	**0,0**	**5,0**	**0,0**	**10,0**
Bimonth 5	**0,0**	**4,0**	**8,0**	**0,0**	**12,0**
Bimonth 6	**0,0**	**0,0**	**6,0**	**0,0**	**6,0**
Total	**10,5**	**6,8**	**43,0**	**0,0**	**60,3**
Expected	**10 - 20**	**5 - 10**	**30 - 45**	**0 – 1.6**	

3. Research activity:

My research activity focused on cybersecurity for IoT devices involved in agri-food application field. In this period, I conducted an in-depth study on the state of the art concerning "side-channel attacks" using "machine learning" models, i.e. attacks on embedded devices based on power traces. I conducted also a with an in-depth study on sustainability of machine learning models embedded into IoT devices instead of use Data Centers that are much less sustainable. I worked on the drafting of a scientific article which is responsible for investigating the performance of side-channel attack using machine learning methods and I also presented a Demo about such attack at 2023 IEEE International Conference On Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering Milan.

4. Research products:

Pasquale Arpaia, Francesco Caputo, Antonella Cioffi, Antonio Esposito, Francesco Isgrò, Uncertainty analysis in cryptographic key recovery for machine learning-based power measurements attacks, IEEE Transactions for Instrumentation and Measurements, 2023

5. Conferences and seminars attended

Demo about practical Side-Channel Attack performed (1) measuring current traces from an IoT device and (2) applying machine learning models to perform the attack. Demo presented at 2023 IEEE International Conference On Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering Milan.

6. Periods abroad and/or in international research institutions

None

7. Tutorship

None

8. Plan for year three

For the third year, is scheduled the period abroad in a STMicroelectronics (France) laboratory site, expert into attack performed on IoT devices, to acquire skills in modern data storage and transmission techniques in a secure and unalterable manner; exploring the embedding of machine learning models into tiny devices to find a way to work without the use of Data Center, much less sustainable than tiny devices. Research will continue by defining the IT security requirements and designing a smart transducer system for green applications, the transducers will be interconnected and will have to implement all identified safety requirements. To this end, modern data manipulation detection techniques will be explored to prevent leaks of sensitive information (e.g. cryptographic keys). Finally, this system will be implemented and will be applied metrologically. The research activities will be accompanied by further training courses and seminars on security and sustainability issues.