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

PhD Student:

Cycle: XXXIX

Training and Research Activities Report

Academic year: 2024-25 - PhD Year: Second

Marco Vorlese

Tutor: prof. Simon Pietro Romano

Simon Pietro Romano

Co-Tutor:

Date: October 21, 25

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: **Author:**

1. Information:

- **PhD student:** Mario Varlese **PhD Cycle:** XXXIX
- **DR number:** DR997197
- **Date of birth:** 13.03.1996
- **Master Science degree:** Computer Engineer **University:** Federico II
- **Scholarship type:** PNRR - DM 118/2023 Dottorati Pubblica Amministrazione (CUP: E66E23001050002)
- **Tutor:** Prof. Simon Pietro Romano
- **Co-tutor:** //
- **Period abroad:** ***list research institutions, public administrations and/or companies and number of months spent/to be spent there***

Entity	Months spent	Months to be spent
Direzione Antimafia e Antiterrorismo	6	0
Universidad Carlos III de Madrid	0	6

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Optimization based Control of Flexible Resources in Sustainable Energy Networks	Seminar	1	0.2	05/02/2025	Prof. Luigi Glielmo	Yes
The Good, The Bad and the Ugly in Quantum Computing: Computational Power, Intrinsic Noise and Transient Faults	Seminar	1	0.2	17/01/2025	Prof. Paolo Rech	Yes
English B2 FCE	Course	48	6	30/09/2024 – 09/12/2024	Dr. Guido Palmitesta	Yes

5G & Digital Transformation: A view from an unconventional perspective	Seminar	4	0.8	14/03/2025	Prof. Antonia Tulino	Yes
Sovranità digitale, cos'è e quali sono le principali minacce al cyberspazio nazionale	Seminar	1	0.2	23/06/2025	Prof. Marcello Cinque	Yes
Trusted execution environments for QPUs	Seminar	1	0.2	27/06/2025	Prof. Edoardo Giusto	Yes
Safety of highly automated driving systems	Seminar	1	0.2	23/04/2025	Prof. Marcello Cinque	Yes
Innovation and Entrepreneurship	Course	24	3	05/06/2025 – 23/07/2025	Prof. Pierluigi Rippa	Yes
Argumentation-Based Reasoning Frameworks for Public Interest Communication in Healthcare	Seminar	2	0.4	29/09/2025	prof. Carlo Sansone, prof. Elio Masciari	Yes
Guardians or Threats? AI at Frontlines of Cybersecurity	Seminar	4	0.8	17/10/2025	Prof. Antonia Tulino	Yes
AI Powered User interface design	Seminar	4	0.8	24/10/2025	Prof. Antonia Tulino	Yes
Quality of services	Seminar	4	0.8	28/10/2025	Prof. Antonia Tulino	Yes
AI Code Generation: Foundations, Evaluation, and Security	Course	24	3	01/10/2025 – 31/10/2025	dr. Pietro Liguori	Yes

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	6	0.4	2.5	0	**8.9**
Bimonth 2	0	0.8	1.8	0	**2.6**
Bimonth 3	0	0.8	1.8	0	**2.6**
Bimonth 4	0	0.4	1.8	0	**2.2**
Bimonth 5	3	0.2	2.5	0	**5.7**

Bimonth 6	0	2	12.2	0	13.4
Total	(45+) 12 = **57**	(5.2+) 5.4 = **10.6**	(18.4+) 22.6 = **41**	**0**	
Expected	**30 - 70**	**10 - 30**	**80 - 140**	**0 – 4.8**	

3. Research activity:

During this second year of my PhD, I continued the collaboration with the National Anti-Mafia and Counter-Terrorism Directorate (DNAA), carrying on the work conducted in the previous year.
I am also exploring the potential of generative artificial intelligence applied to the field of cybersecurity.
In addition, I contributed to advancing some activities with my research group. The activities are detailed below.

National Anti-Mafia and Counter-Terrorism Directorate

The reengineering of existing processes requires a detailed understanding of how they function in order to analyze potential intervention points and inefficiencies, and to subsequently integrate new technologies. Business process modeling using Business Process Modeling Notation (BPMN) is commonly employed in these contexts.

It aims at redesigning processes to eliminate redundancy, reduce resource consumption, and achieve substantial improvements in efficiency, effectiveness, and adaptability in organizations and public administration.

Recent advances in Natural Language Processing (NLP), and in particular in Large Language Models (LLMs), enabled the full or partial automation of tasks that previously required human intervention (e.g., information extraction), contributing to the optimization of existing business processes. In this context, I examined the current processes of “Direzione Nazionale Antimafia e Antiterrorismo” (DNAA) and “Direzione Distrettuale Antimafia” (DDA) regarding the knowledge extraction and analysis of documents produced during investigative phases.

This analysis led me to detect inefficiencies by modeling current and future workflows through BPMN, while ensuring strict privacy requirements and aligning with the ethical guidelines highlighted by the European Commission. This activity resulted in the proposal of a hybrid architecture that leverages a fine-tuned LLM for Named Entity Recognition (NER), combined with a pipeline of steps employing static rules and an LLM for Relationship Extraction (RE). In particular, I focused on legal criminal procedures (e.g., interrogation records, search reports, and seizure reports), which are characterized by highly intricate linguistic structures.

Generative AI for Security

Software exploitation is the process of taking advantage of vulnerabilities in software systems in order to perform unintended activities. Its understanding leads to improved defensive measures and informed decision making about which security mechanisms to prioritize. However, creating a software exploit is typically a time-consuming and manual task that demands a deep understanding

of programming, network protocols, operating system internals, and computer architectures. Additionally, it requires the ability to integrate this knowledge through complex reasoning and problem-solving techniques.
In recent years, the emergence of Large Language Models (LLMs) has offered unprecedented possibilities for automating complex tasks that have traditionally relied upon human expertise. These models, which have been trained on vast datasets, unveil the potential for understanding and generating remarkably accurate natural language text.
Given these premises, I have recently explored the effectiveness of using LLMs in the generation of buffer overflow vulnerability exploits.
The proposed solution is based on a fully automated system that leverages two specialized LLMs, enabling structured exploit generation through an FSM-driven approach.
Other ongoing activities aim at the use of these models, employed using different architectures (workflow-based or agent-based) for the automation of phases of penetration testing. At the moment, I am investigating the use of LLMs—both workflow-based and agentic architectures—to automate stages of penetration testing. My primary goal is to evaluate whether an LLM-based system can generate a valid exploit from a CVE description. All work will be carried out under strict ethical and legal constraints, in controlled test environments, and with measures to prevent misuse.

AKADIMOS

The increasing complexity of cyber threats and the widening skills gap in Europe underscore the urgent need for a clear and flexible strategy for the cybersecurity workforce. Many projects have tried to address these problems. Though, despite their relevant contributions, divergent directions were followed, thereby reinforcing the need for a harmonized and standard approach. The European Cybersecurity Skills Framework (ECSF) represents a significant step in this direction, but its adoption poses several challenges. It is therefore particularly valuable to examine the structural differences and interdependencies between the ECSF and other frameworks in order to assess their respective strengths, complementarities, and potential for mutual enhancement. This poses the basis of our study, namely, to analyze the ECSF through the lens of related frameworks in order to identify limitations and formulate enhancement strategies. We show that through a detailed analysis of the contributions made by related works, it is possible to identify areas for improvement that will empower the ECSF, thereby supporting the development of a shared, structured understanding of roles, skills, and knowledge essential for strengthening the European cybersecurity workforce. This work is conducted in the context of the AKADIMOS project, a European initiative supporting the establishment and operation of the Cybersecurity Skills Academy, with the goal of enhancing the ECSF and contributing to a coordinated effort to bridge the cybersecurity skills gap across the EU.

4. Research products:

- Perrone, G., d'Ambrosio, N., D'Isanto, R., Rak, M., Russo, L., Romano, S. P., Varlese, M. (2025). One Europe, One Framework: aligning ECSF with global standards through the AKADIMOS Initiative. *[pending submission*]
- Romano, S. P., Sperlì, G., Varlese, M., Vignali, A. (2025). Integrating BPR and LLMs for Enhanced Workflow Management in Criminal Investigation. [*pending submission*]
- Romano, S. P., Sperlì, G., Varlese, M., Vignali, A. (2025). NER in the Courtroom: A Data-Driven Framework for Legal Entity Extraction. *Information Processing & Management*, [*submitted*]
- Caturano, F., Ciotola, J., Romano, S. P., & Varlese, M. (2025). A chit-chat between Llama 2 and ChatGPT for the automated creation of exploits. *Computer Networks*, 111501. [*published*]

5. Conferences and seminars attended

//

5. Periods abroad and/or in international research institutions

- Research activities described above have been carried out by collaborating with "*Direzione Nazionale Antimafia e Antiterrorismo" (DNA).* Several meetings and discussions were conducted to understand their actual systems in the context of the refactoring of their database, "*Banca Dati Nazionale*" (BDA). Our main objective was to demonstrate the applicability of cutting-edge technologies to their processes through a prototypal development approach. Below are detailed the periods.
    - May – June 2024
    - October – November 2024
    - February – March 2025

- Abroad research period at the University of Madrid, Carlos III , under the supervision of Prof. Juan Manuel Estévez Tapiador. The internship will start on January 2026 and the duration will be six months.

7. Tutorship

//

8. Plan for year three

In the next year, I plan to:

- Continue the exploration of the Generative AI in the field of the Cyber Security;
- Contribute to the European project AKADIMOS to complete the defined deliverables;
- Spend six months at University Carlos III, Madrid, under the supervision of the Prof. Juan Manuel Estévez Tapiador;
- Co-supervise master students;
- Write my thesis on AI techniques to cybersecurity