PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

Ph.D. Student: Luciano Pianese

Cycle: XXXIX

Training and Research Activities Report

Academic year: 2024-25 - PhD Year: Second

Tutor: prof. R. Natella

Co-Tutor: BRACCIOLI Marco

Date: October 31, 2025

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX **Author: Luciano Pianese**

1. Information:

- **PhD student:** Luciano Pianese
- **DR number:** DR997206
- **Date of birth:** 08/10/1998
- **Master Science degree:** Computer Engineering
- **University:** Università degli Studi di Napoli Federico II
- **Doctoral Cycle:** XXXIX
- **Scholarship type:** PNRR - DM 117/2023
- **Tutor:** Roberto Natella
- **Co-tutor:** Marco Braccioli
- **Period abroad:** The Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg, 6 months.

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
AI and Enabling Technologies for Social Robots	**Seminar**	**2**	**0.4**	**03/12/2024**	**Prof. Franco Cutugno**	**Y**
Strutture basate su regole e strutture basate su approssimazioni	**Seminar**	**2**	**0.4**	**10/12/2024**	**Prof. Franco Cutugno**	**Y**
Strutture basate su regole e strutture basate su approssimazioni	**Seminar**	**4**	**0.8**	**14/03/2025**	**Prof.ssa. Antonia Maria Tulino**	**Y**
On the Security of Semantic Watermarking to Detect AI-Generated Content	**Seminar**	**1**	**0.2**	**29/04/2025**	**Prof.ssa Luisa Verdoliva**	**Y**
IELTS Advanced Preparation course	**Course**	**50**	**6**	**16/09/2024-16/12/2024**	**Centro Linguistico di Ateneo**	**Y**

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	0	0.8	9.2	0	10
Bimonth 2	0	0	10	0	10
Bimonth 3	6	1	3	0	10
Bimonth 4	0	0	10	0	10
Bimonth 5	0	0	10	0	10
Bimonth 6	0	0	9	1	10
Total year	6	1.8	51.2	1	60
Total global	32	10.2	76.8	1	120
Expected	30 - 70	10 - 30	80 - 140	0 – 4.8	

3. Research activity:

The research conducted during this second year of doctoral studies remains focused on the "offensive security" procedures automation using generative artificial intelligence (AI).
To clarify, "Offensive security" refers to all those methodologies in cybersecurity that try to address sophisticated and structured cyber attacks, such as the "Advanced Persistent threats" (APTs), by proactively taking defensive actions before the effective occurrence of the attack; for instance, one technique called "Threat Emualtion" simulate the behavior of a cyber attack campaign over an emulated enviroment to analyze and assess the posture of the real cyber infrastructure against it.
Although the strength of those approaches has been made evident compared to the traditional one (reactive security), they remain unused due to:

- The lack of specialized expertise.
- The enormous necessity in terms of expert resource demands.

Consequently, Generative AI has found its way in automating these procedures, providing supporting capabilities to the domain experts.
The undertaken studies examined how Generative AI can automate three distinct areas within Offensive Security:

- Engineering and evaluation of AI-Generated Malware in a post-compromised scenario
- Automation of Defence Action through Agentic AI paradigm
- Automation of Thread Emulation procedures, providing human-labeled datasets

Malware generation and evaluation

This first contribution extends the previously conducted research, addressing the final stage of the Threat Emulation chain, where Cybersecurity professionals evaluate the effectiveness of cyberattacks generated via Large Language Models (LLMs).
In particular, this work aims to construct a methodology to:

- Generate complete cyber-attacks written in PowerShell starting from a natural language description
- Evaluate a complete generated cyber-attack.

The methodology encompasses the development of Algorithms capable of generating Malware through standardized procedures such as Training, fine-tuning, and prompt engineering. The construction of Human-labeled datasets. Finally, the design of the evaluation procedures.

Agentic AI for Incident Response Procedures

Agentic AI represents a new paradigm in the field of AI. Hence, it is a promising solution to automate complex offensive security tasks and reduce reliance on scarce human expertise. By leveraging multiple LLMs, agentic frameworks are capable of multi-step reasoning and autonomous decision-making, to orchestrate tools, to refine strategies iteratively, and to emulate attacker behaviors in a scalable way.

This contribution, in partnership with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), intends to develop procedures and support tools that apply the Agentic AI paradigm to structure an Incident response plan against APT attacks.

Threat Emulation dataset

The latter contribution involves the Cyber Threat Intelligence (CTI) field and comprises the design and construction of structured and human-labeled data extracted from human-written, unstructured Incident Reports, which are the most common medium of APT information.

Those data are pivotal to building methodologies for:

- Supervised data preparation
- Automation of information retrieval
- Constructing autonomous systems for Threat emulation procedures

Methodologies that will be addressed in future works.

HPC Application Projects

Conducting experimental research on LLMs demands substantial computational resources. To access such resources, grant applications were prepared and submitted to the *Italian SuperComputing Resource Allocation* (ISCRA), the national allocation program managed by CINECA.

These grants are awarded through a selection process carried out to evaluate the scientific relevance and technical feasibility of each proposal

In collaboration with CINECA, I have served as co-Principal Investigator in the following two ISCRA projects:

- *Generative AI for Offensive Security* (Ge-OS)
- Agentic woRkflows and Generative AI for Offensive Security (ARGOS)

4. Research products:

Della Penna, S., Natella, R., Orbinato, V., Parracino, L., & **Pianese, L**. (2025). CTI-HAL: A Human-Annotated Dataset for Cyber Threat Intelligence Analysis. - Workshop on Attackers and CybeCrime Operations (WACCO)

5. Conferences and seminars attended

None

6. Periods abroad and/or in international research institutions

Abroad period at The Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg (Luxembourg) starting from 15/01/2025 to 15/07/2025 – 6 months. Supervised by Ph.D. Antonio Ken Iannillo.
Cooperation with the partner company lasted:

- 2 Months, November to December 2024
- 2 Months, September to October 2025

7. Tutorship

1 Credit earned in tutorship for BSc. Course "Operating Systems", preparing programming exercises assigned to student to explain the correct usage of POSIX APIs, and explaining them the solution.

8. Plan for year three

The concluding year of the Ph.D. program will prioritize the dissemination of current findings and the extension of ongoing work. Supportive academic activities, including tutoring, will proceed throughout the next year. The thesis will culminate in a thorough assessment of offensive security practices through the usage of the Agentic AI paradigm.