UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

itee PhD
information technology
electrical engineering

Mario Varlese

Tecniche 'offensive' per migliorare la sicurezza informatica delle pubbliche amministrazioni

Tutor: Prof. Simon Pietro Romano

Cycle: XXXIX Year: Second

itee PhD
information technology
electrical engineering

Background

- MSc degree in Computer Engineering from University of Naples Federico II
- DIETI Research group/laboratory: Computer Networks and Architectures Laboratory (ARCLAB)
- PhD start date: 01/11/2023
- Scholarship type: PNRR - DM 118/2023 Dottorati Pubblica Amministrazione (CUP: E66E23001050002)
- Internship
  - Direzione Nazionale Antimafia ed Antiterrorismo (DNAA)
  - University of Madrid Carlos III (six months starting from February 2026)
- Ad hoc PhD courses:
  - Innovation and Entrepreneurship
  - English B2 FCE

Research field of interest

I have worked extensively with large language models (**LLMs**) for information extraction (IE) tasks—specifically named-entity recognition (**NER**) and relation extraction (RE)—developing pipelines that structure **complex legal and investigative data**.

My **current interest** focuses on **cybersecurity**:

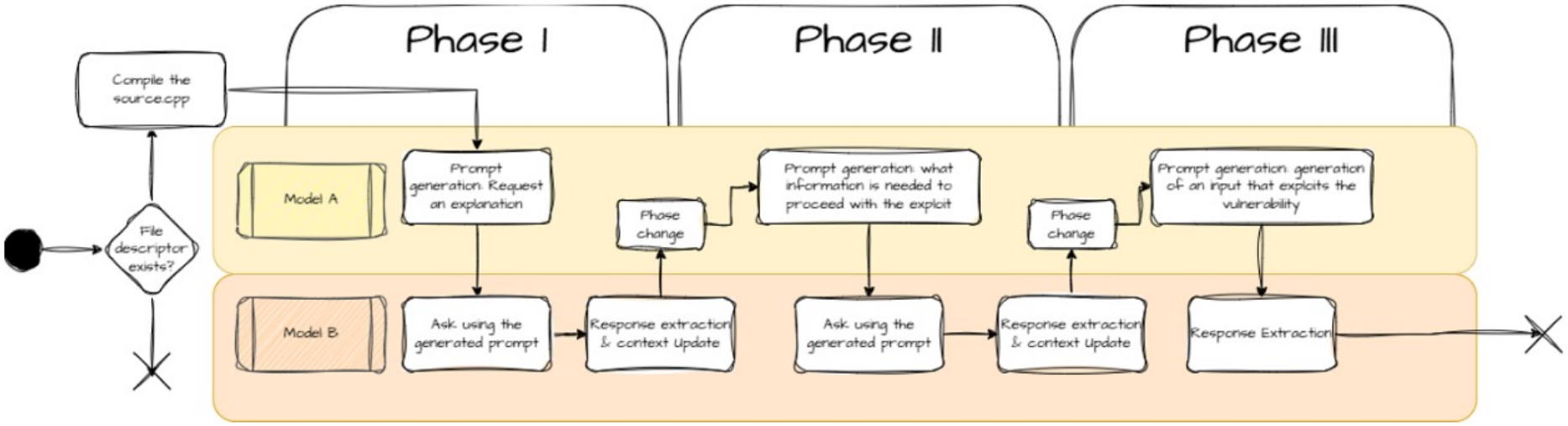
- Exploit Automation: *Exploring how generative and reasoning-based AI can be employed to **automate** or simulate **adversarial actions** – such as for the exploit generation.*
- AKADIMOS: *Ongoing contribution to identify the applicability limitations of the European Cybersecurity Skills Framework (**ECSF**) and to address its extension within the European AKADIMOS project*

Research activity: Exploit Automation

- *Context:* Exploration of Large Language Models (LLMs) for automating complex cybersecurity tasks, focusing on exploit generation as a proof-of-concept research study ("A chit-chat between Llama 2 and ChatGPT for the automated creation of exploits").
- *Problem:* Manual exploit creation is time-consuming and requires deep technical expertise; the goal is to assess whether an LLM-based system can autonomously generate valid exploits.
- *Objective*: My primary goal is to evaluate whether an LLM-based system can generate a valid exploit for Buffer Overflow vulnerabilities.

Research activity: Exploit Automation

- *Methodology*: Development of a fully automated, FSM-driven system leveraging two specialized LLMs for structured buffer overflow exploit generation.

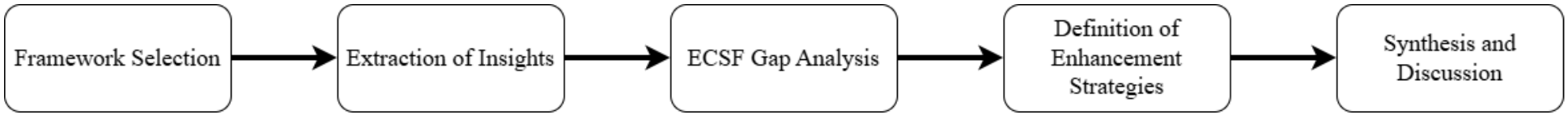


Research activity: AKADIMOS

- *Context:* The increasing complexity of cyber threats and the widening skills gap in Europe require a clear and flexible strategy for the cybersecurity workforce. The AKADIMOS project supports the establishment and operation of the Cybersecurity Skills Academy, aiming to strengthen skills and harmonize European standards.
- *Problem:* Adoption of the European Cybersecurity Skills Framework (ECSF) faces challenges with the diverse requirements of stakeholders from public institutions, industry, and academia.
- *Objective:* Analyze the ECSF through the lens of related frameworks to identify limitations, assess strengths and complementarities, and formulate enhancement strategies to improve the framework, making its adoption easier.

Research activity: AKADIMOS

- *Methodology:*
  - Conduct a detailed in-depth comparative analysis of ECSF and related frameworks, highlighting structural differences, interdependencies, and potential areas for improvement.



  - Define a methodology to map Courses and Certifications to the extended ECSF.
  - Develop surveys to evaluate the effectiveness of the mapping methodology.

Products

[P1]	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*]
[P2]	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*]
[P3]	Romano, S. P., Sperlì, G., Varlese, M., Vignali, A. (2025). Integrating BPR and LLMs for Enhanced Workflow Management in Criminal Investigation. [*pending submission*]
[P4]	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*]

Next year

- 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 Prof. Juan Manuel Estévez Tapiador;
- Co-supervise master students;
- Write my thesis on AI techniques for cybersecurity