COESIONE ITALIA 21-27 PIEMONTE

Cofinanziato dall'Unione europea

REGIONE PIEMONTE

Intervento realizzato da

Politecnico di Torino

ScuDo Scuola di Dottorato – Doctoral School WHAT YOU ARE, TAKES YOU FAR

In consideration of the determination of the Regione Piemonte – Direzione Istruzione, formazione e lavoro No. 218 of 2022, May 3 which listed the higher institutions authorized to activate PhD positions in the apprenticeship format for the years 2022-2024 in the framework of a specific regional call for proposals (Apprendistato di Alta Formazione e Ricerca - Avviso Pubblico 2022-2024 per l'individuazione e la gestione dell'offerta formativa pubblica approvato con Determinazione 114 del 3/3/2022 e s.m.i.)

COMPUTER AND CONTROL ENGINEERING

AI-driven cybersecurity assessment for automotive

Company	Drivesec s.r.l. [P.iva/CF:11773810012]
Supervisor	CAGLIERO LUCA - luca.cagliero@polito.it
Contact	Giuseppe Faranda Cordella (email: gfc@drivesec.com)
Context of the research activity	This PhD proposal aims to investigate how to leverage Generative AI for assessing the cybersecurity posture of vehicles and automotive infrastructures and evaluating the compliance with existing standards. It will propose innovative LLM-based approaches to retrieve and generate penetration tests and vulnerability-related information. The Company Drivesec has planned for the winner of this position a collaboration within a contract of high apprenticeship according to the Italian Legislative Decree 81/2015, art. 45.
	Research objectives Assessing the resilience of vehicles and their components has become crucial; it relies on tests that decree the security of a System Under Test. Vulnerability assessment (VA) and penetration testing (PT) are two primary complementary techniques that serve this purpose. VA is managed with automatic tools, but the existing ones rarely work in the automotive field. PT relies on teams made humans, which are costly and difficult to hire. Hence, the aim of this research is to investigate how the advancements in AI techniques can help automate the threat assessment and risk evaluation for

Objectives

the automotive field. The PhD candidate will investigate innovative methods for the automatic processing and interpretation of the data produced by the analysis tools in their context, understand the implications from the security point of view, and use them to build a risk analysis model. Moreover, the PhD candidate will explore the potential of Generative AI techniques, in combination with Search Engines, Question Answering models, and Multimodal Learning architectures to automate the process of retrieval, recommendation and generation of penetration tests.

Outline

The PhD candidate will get familiarity with the field of cybersecurity for automotive, the peculiarities and the normative framework. His main research goal is to leverage Generative AI to model VA/PT operations and generate new tests for assessing the verification objectives and adapting family of tests to work out of their original context. To this end, the algorithms, models, and techniques considered in the research activities will include (but are not limited to):

- Large Language Models (e.g., GPT [1], Llama 2 [2], Llava [3]), to leverage the capabilities of transformer-based generative models to interpret end-users' questions posed in natural language, generate text and code that meet in-context requirements, and perform multi-hop reasoning based on Chain-of-Thought (CoT) Prompting;
- Multimodal Architectures (e.g., CLIP [4]), to effectively handle input data in different modalities (e.g., images, tables, speech);
- Search engines (e.g., ElasticSearch [5]), to efficiently store, index, and retrieve data about vulnerabilities and penetration tests;
- Retrieval-Augmented Generation (e.g., Llama Index [6]), to efficiently address question answering tasks on proprietary data by leveraging LLM capabilities.

Industrial collaborations

This research will be made in collaboration with Drivesec s.r.l., which will provide the necessary automotive background, the equipment needed, and the data set for the testing and validation of the developed methods.

Open resources

Beyond proprietary data and industrial case studies, the PhD activities will also consider opensource data repositories, models, and projects, e.g.,

- MetaSploit (https://www.metasploit.com/)
- MITRE (https://cve.mitre.org/)
- PentestGPT (https://github.com/GreyDGL/PentestGPT)
- HuggingFace (https://huggingface.co/models).

List of possible publication venues

- Conferences: IEEE CSR, ECML PKDD, ACM CIKM, KDD, IEEE ICDE, IEEE ICDM
- Journals: IEEE TKDE, IEEE TAI, ACM TIST, IEEE TIIS, IEEE/ACM ToN, Elsevier Information Sciences, Elsevier Computers in Industry.

References

[1] OpenAI: GPT-4 Technical Report. CoRR abs/2303.08774 (2023)
[2] https://ai.meta.com/llama/
[3] Hao Zhang, Hongyang Li, Feng Li, Tianhe Ren, Xueyan Zou, Shilong Liu, Shijia Huang, Jianfeng Gao, Lei Zhang, Chunyuan Li, Jianwei Yang: LLaVA-Grounding: Grounded Visual Chat with Large Multimodal Models. CoRR

	abs/2312.02949 (2023) [4] https://openai.com/research/clip [5] https://www.elastic.co/) [6] https://www.llamaindex.ai/

Skills and competencies for the development of the activity	The candidate shall be less than 30 years old at the moment of the hiring from the company. The skills of the candidate imply competences in: - ability to critically analyze complex systems, model them and identify weaknesses; - proficient Python programming; - knowledge about cybersecurity fundamentals; - a solid background on machine learning and deep learning; - natural inclination for teamwork; - proficient English speaking, reading, and writing. Motivated candidates who are willing to work at the intersection between academia and industry are preferred.