AI4SIM

LLM-based attack generator

An LLM-based solution to automatically generate executable code that aligns with the atomic tactics, techniques and procedures (TTPs) defined in the MITRE ATT&CK model, specifically the MITRE ATT&CK Enterprise version.

AI4CYBER Component

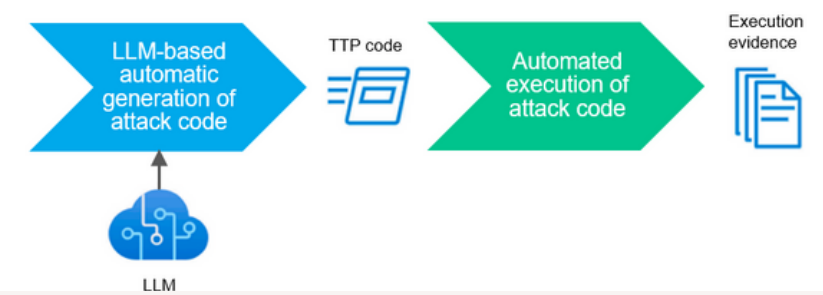
The main benefit of the solution is the automation of the creation of staged and complex attacks combining several TTPs. The attack simulation automation eases the testing of the system against multiple types of attacks, e.g., in pentesting. The solution allows non-skilled security professionals with limited attack knowledge to create advanced threat simulations

The LLM-based attack technique generator by TECNALIA is a python prototype that allows the automatic creation and execution of diverse attack technique codes.

The generated TTP code adheres to the TTPs defined in the MITRE ATT&CK Enterprise framework, which is the world-wide de-facto standard for TTPs taxonomy. The LLM leveraged by the subcomponent is OpenAI's GPT v3.5, since the solution was started at the time of publication of GPT 3.5. In the near future it is planned to use higher versions of GPT for more accurate generation of the code pieces.

The solution includes two main functionalities: the TTP code generation, where a new code for a specific TTP selected by the system security operator is generated thanks to the automatic request to the LLM, and the TTP code execution which is responsible to execute over the system under test the new TTP code generated and execute it over the system selected by the system security operator.

The tool has been tested by running the automatically generated TTP codes against multiple hosts characterized by different platforms (linux and Windows) and operating system versions.



The solution is still a prototype and the future tool will have commercial license.

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Erkuden Rios (Erkuden.rios@tecnalia.com)
Fundación Tecnalia Research & Innovation

www.tecnalia.com
https://es.linkedin.com/company/tecnalia-research-innovation
https://x.com/tecnalia

- E. Iturbe, O. Llorente-Vazquez, A. Rego, E. Rios, y N. Toledo, "Unleashing offensive artificial intelligence: Automated attack technique code generation", Comput. Secur., vol. 147, núm. 104077, p. 104077, 2024. (https://www.sciencedirect.com/science/article/pii/S0167404824003821)
- E. Iturbe, E. Rios, A. Rego, and N. Toledo, "Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework", in Proceedings of the 18th International Conference on Availability, Reliability and Security, 2023, pp. 1–8.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450. Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.