Master Thesis: LLM Agents in Penetration Testing

Robert-Bosch-Allee 1, 74232 Abstatt, Deutschland
Legal Entity: Robert Bosch GmbH

Company Description

Would you like to turn your ideas into practical and useful technologies? Whether in Mobility Solutions, Consumer Goods, Industrial Technology or Energy and Building Technology - with us you will improve the quality of life of people all over the world. Welcome to Bosch.

Robert Bosch GmbH is looking forward to your application!

Introduction

In an era where cybersecurity threats are increasingly sophisticated, the automation of penetration testing presents a pivotal opportunity for enhancing product (ECUs – electronic control units) defenses. This thesis explores the innovative potential of Language Learning Model (LLM) agents in automating penetration testing, focusing on both routine and creative aspects. By examining how agents can collaborate and adapt to real-world scenarios (CAN and/or Ethernet), this research aims to uncover new strategies for safeguarding digital communication channels. It seeks to balance the benefits of automation with the associated risks, providing a comprehensive perspective on the future of cybersecurity.

Description

The proposed thesis aims to investigate the role of Language Learning Model (LLM) agents in the automation of penetration testing within corporate environments. Initially, the student will identify the distinct steps involved in penetration testing of communication channels and explore how these can be automated. The focus will be on developing streamlined processes that not only form part of standard penetration testing but could also be exploited by potential attackers. These processes will be tailored to real-world products, examining the collaborative capabilities of agents necessary for conducting effective automated tests.

This research will move beyond the mere automation of typical penetration testing steps. It will delve into how agents can enhance the creative aspects of penetration testing. Specifically, it will explore the potential for agents to adapt and modify data based on project-specific information or interaction with other agents, thereby generating novel test cases and strategies.

A critical component of this thesis will be the assessment of risks associated with the use of agents for automation, particularly when significant automation is achieved. This includes evaluating the dangers posed by agent hallucinations, where agents may misinterpret information or execute incorrect actions.

In summary, this thesis aims to provide a comprehensive analysis of the feasibility of automating penetration tests with LLM agents. It will highlight both the opportunities and risks associated with this approach, focusing on enhancing both routine and creative processes for penetration testers through effective automation.

Qualification

- Personality:
  - motivated, responsible
  - self-confident, flexible, able to moderate.
  - able to work in a team and with good communication skills.
- Working style:
  - independent, self-reliant, structured, analytical, and confident in dealing with other business units.
- Experience and Know-How
  - knowledge in security engineering & testing
  - experience with LLM
  - ideally experience with Python
- Language: very good communication and language skills in English
- Education: current studies in the field of computer science, engineering, or comparable studies