CARIAD Master Thesis- AI Usage in CI/CD/CT Pipelines for Compute Platforms in Automotive

Introduction

In recent years, software development has changed dramatically. We've seen a huge increase in the complexity of software systems, and at the same time, there's a growing demand for faster development cycles. To keep up with this, methodologies like Continuous Integration (CI), Continuous Delivery (CD), and Continuous Testing (CT) pipelines have become essential. These pipelines help automate and streamline the entire process of developing software, allowing teams to deliver high-quality results more efficiently. This is particularly important in industries such as automotive, where software plays a critical role in controlling essential functions, so safety and reliability are absolutely paramount.

However, this increased complexity also brings new challenges, especially when it comes to ensuring software security. Traditional security testing methods often struggle to keep pace with the speed at which new features are developed and deployed, which can create potential vulnerabilities. Fortunately, Artificial Intelligence (AI) and Large Language Models (LLMs) offer promising solutions. They can enhance the automation, effectiveness, and overall intelligence of security testing within these CI/CD/CT pipelines.

Overview

The primary aim of this thesis is to explore and implement AI-driven solutions within Continuous Integration (CI), Continuous Delivery (CD), and Continuous Testing (CT) pipelines, specifically focusing on Whitebox fuzzing techniques for automotive compute platforms. This research will investigate the integration of Artificial Intelligence (AI) and Large Language Models (LLMs) to enhance the automation and effectiveness of security testing within CARIAD's development environment.

This master thesis proposal outlines a project that will also focus on the development of automated systems for generating test artifacts, such as test cases, test procedures, and test reports, based on the results of AI-driven fuzzing. The practical implementation within CARIAD will provide valuable insights and potentially contribute to the improvement of their software development and security assurance processes.

Research Objectives

- Investigate and develop novel security testing methods that integrate Whitebox fuzzing techniques with the capabilities of LLMs and AI. The main focus is on Whitebox fuzzing.
- Define and implement the identified security testing into an existing or proposed Continuous Integration/Continuous Delivery/Continuous Testing (CI/CD/CT) pipeline.
- Develop mechanisms for the automatic generation of test cases, test procedures, test reports, and a product quality matrix based on the results of the implemented security testing methods.
- Explore and analyze techniques for the automatic generation of realistic and effective mock scenarios to enhance the scope and effectiveness of security testing.
- Analyze the impact of the implemented AI-driven security testing methods on key performance indicators such as test run time, efficiency in identifying vulnerabilities, and overall test coverage.

Expected Outcomes

- A well-researched and developed approach for integrating AI and LLMs into Whitebox fuzzing techniques for automotive software security testing.
- A proof-of-concept practical implementation of these methods within a CI/CD/CT pipeline, demonstrating their feasibility and effectiveness.
- An automated system for generating comprehensive test artifacts (test cases, procedures, reports, quality matrix) based on the results of AI-driven fuzzing.
- Insights into the challenges and benefits of automatically generating mock scenarios for security testing in the automotive context.
- Assessing the impact of these AI-driven techniques on the efficiency, coverage, and time effectiveness of security testing.
- A quantitative analysis of the impact of these AI-driven techniques on the best way to do continues fuzzing and estimation for exit criteria.

The findings of this thesis will contribute to the advancement of security testing practices in the automotive industry, specifically by exploring innovative ways to leverage AI and LLMs for enhanced automation and vulnerability detection.