

LLM-introduced Supply Chain Insecurity

Advisor: **Moritz Waser**

Motivation

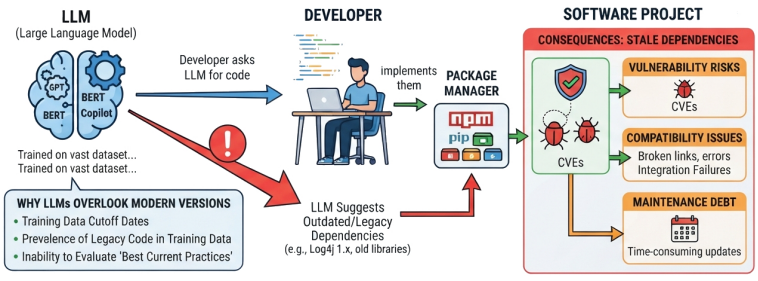
Agentic AI is increasingly used to automate and accelerate administrative tasks such as infrastructure development. Developers routinely let large language models (LLMs) generate configuration files like Dockerfiles, CI pipelines, or dependency manifests. However, these LLM-generated configurations often pin stale or heavily outdated software versions, such as end-of-life base images or packages with known vulnerabilities. Even worse, dependencies might be entirely hallucinated [1]. As a result, LLMs can silently introduce insecure dependencies into the software supply chain.

This Project

This project aims to systematically measure how LLMs handle dependency management and how often they introduce outdated or vulnerable software. Based on these findings, the project explores prompt engineering techniques to improve on the current state of the art.

Goals and Tasks

- Conduct a large-scale study of LLM-based dependency management
- Analyze frequent pitfalls in LLM-generated configurations
- Improve the state of the art through prompt engineering and harness development



LLM-based software lifecycle.

Literature

- J. Spracklen et al.
  We have a package for you! a comprehensive analysis of package hallucinations by code generating LLMs
  Proceedings of the 34th USENIX Conference on Security Symposium

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in software supply chain security
- Interest in LLMs and agentic AI
- Programming (Python)
- Familiarity with Docker and containerization

Advisor Contact

moritz.waser@tugraz.at