DEOBFUSCATOR

Usecase Speicification

2025.04.20

202002514 안상준
202202602 손예진
202202487 박혜연
조은선 교수님

Contents

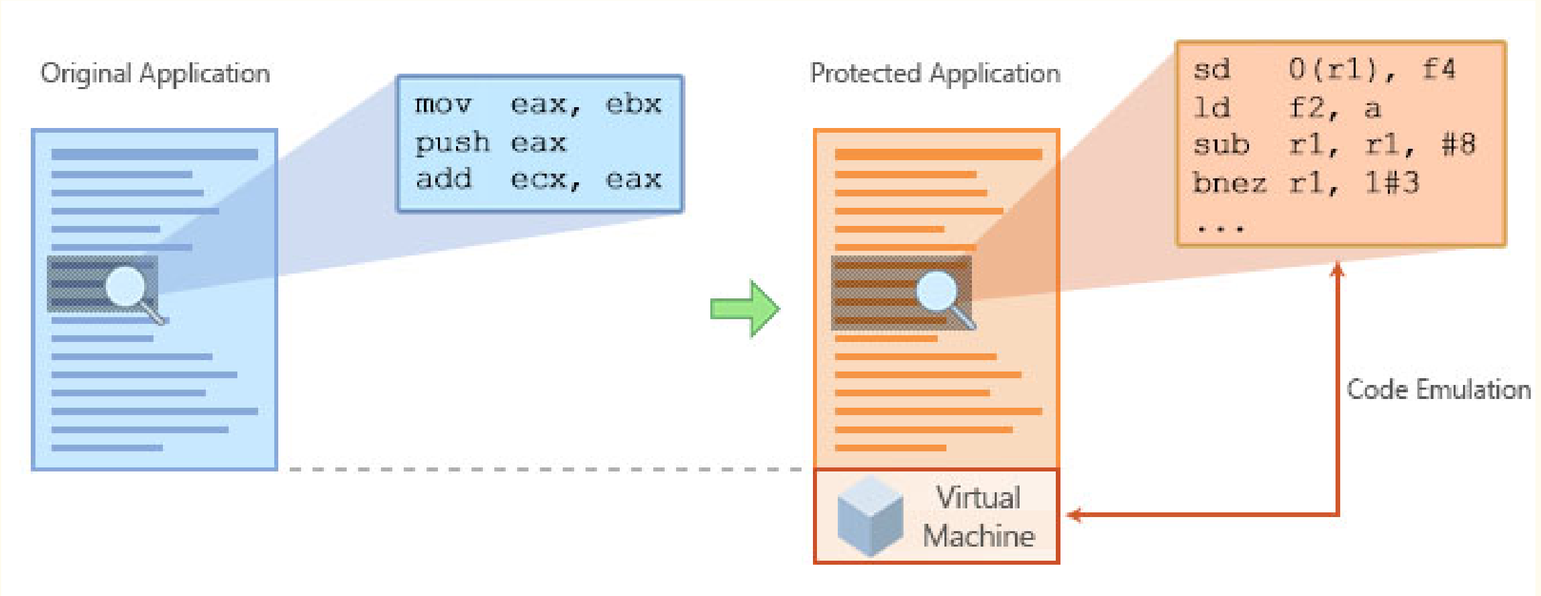
01 배경 / 목적

연구 배경

점차 증가하는 악성코드로 인해 이를 분석할 도구의 필요성이 대두되고 있다. 악성코드는 주로 난독화가 되어 있고 사용한 기법도 다양하여 분석하는데 어려움이 있다.
이는 AI를 활용하여 해결할 수 있지만 보안 분야에서 LLM은 신뢰성이 부족하여 사용되지 못하고 있다.

연구 목적

다양한 난독화 기법이 적용된 VM난독화 코드를 역난독화 하는 연구를 지원하는 LLM기반 모델을 개발하고자 한다.
다양한 난독화 기법이 적용된 코드의 구조를 분석하며 기상화 난독화 코드의 구조인 loop-switch 구조를 LLM을 이용하여 식별하는 것을 목표로 한다.



02 연구 질문 / 가설

질문

RQ1.
LLM기반 loop-switch제어구조 탐지가 가상화난독화 역난독화 연구의 정확도 및 신뢰성 향상에 어떠한 영향을 미치는가?

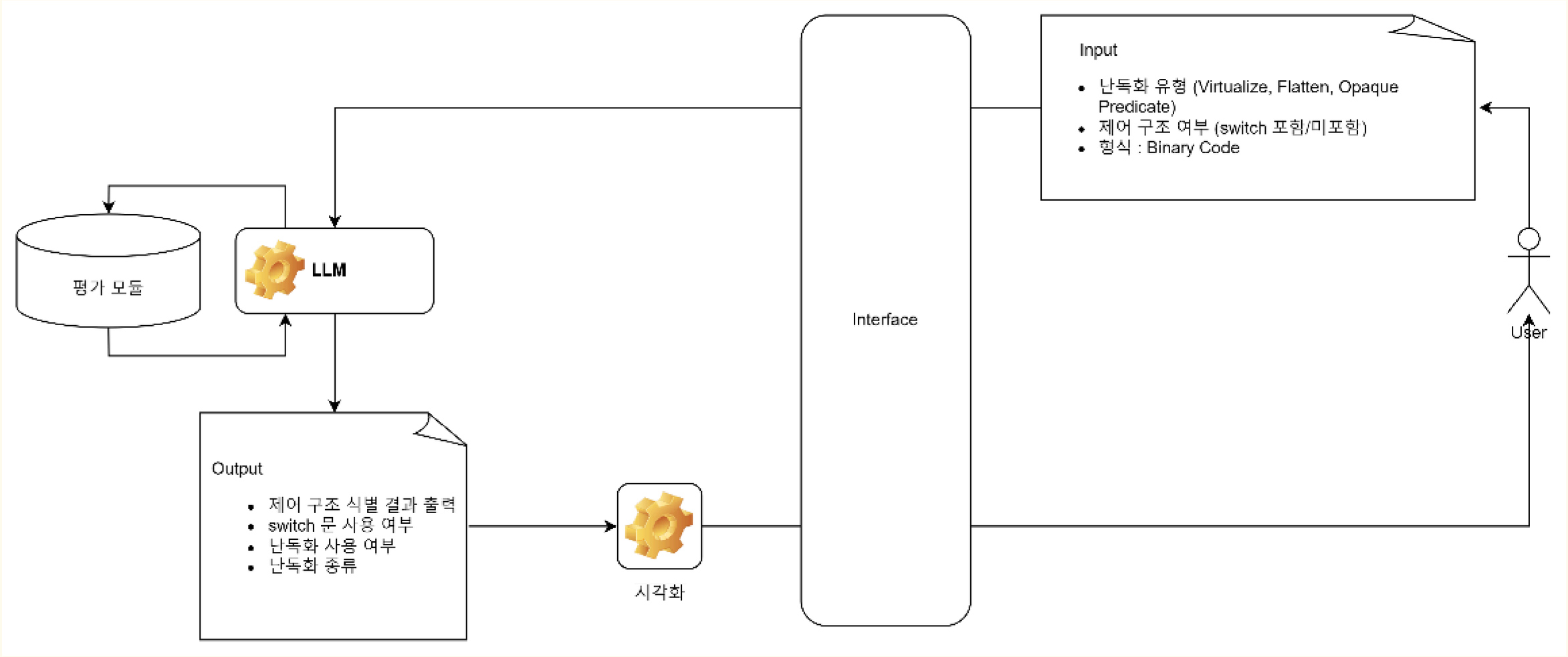
RQ2.
LLM에 fine-tuning 혹은 few-shot prompting을 통해 구성된 제어구조 식별 도구는 다양한 난독화 기법(flattening, opaque predicate 등)에 따라 분석 성능에 차이를 보이는가?

가설

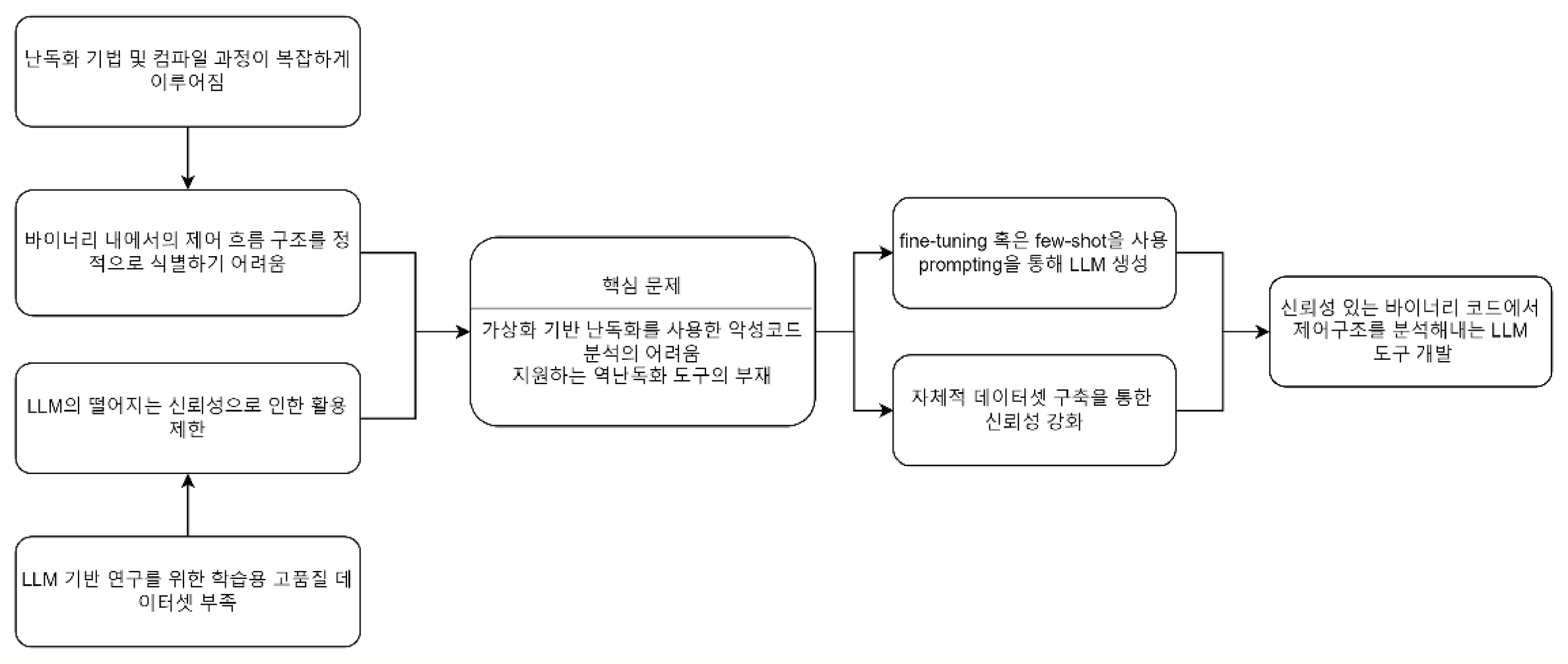
H1.
가상화 난독화 구조인 fetch-decode-execute 구조를 식별함으로써 코드의 원래 흐름과 구조를 분석하는데 큰 도움이 될 것으로 예상한다.

H2.
다양한 데이터셋을 이용하여 LLM에 fine-tuning 또는 few-shot prompting을 통해 학습시킨다면, 여러 난독화 기법에 유연하게 적용이 가능할 것으로 보인다.

03 Usecase Diagram



04 문제 해결에 대한 사용 사례 Diagram



05 소프트웨어 활용 사례

주요 기능

LLM을 사용하여 Binary Code의 제어 구조(loop-switch)를 식별하여 역난독화 및 코드 분석 지원

구성 요소

난독화 유형에 관계없이 제어 흐름 정보를 추출할 수 있도록 LLM 활용

06 문제 해결에 대한 사용 사례

가상화 기반 난독화를 사용한 악성코드의 분석의 어려움과 이를 지원하는 역난독화 도구의 부재

다양한 난독화 기법에 대응하기 어려움
LLM의 낮은 신뢰성

새로운 난독화 기법의 개발
LLM 학습용 고품질 데이터셋의 부족

LLM기반 자동화 분석 및 탐지로 인한 효율 향상
향후 가상화난독화 역난독화 연구 지원

07 AI 도구 활용 정보

사용 도구	GPT-4-turbo
사용 목적	연구 질문 작성, 데이터 Flow 작성, 활용 맥락 작성
프롬프트	● 연구 질문에 대한 예시를 작성해줘 ● 입력 데이터와 출력 데이터 등을 바탕으로 데이터 Flow 어떤식으로 이루어질지 작성해줘 ● 우리 연구의 결과가 어떤 맥락에서 활용될 수 있는지 작성해줘
반영 위치	1. 연구 질문/가설 (p.6) 2. 소프트웨어 활용사례 (p.8) 3. 문제 해결에 대한 활용 사례 (p.9)
수작업 수정	있음(논리 보강, 사례 교체 등 Gpt가 작성한 초안에 대한 수정)

DEOBFUSCATOR

감사합니다

202002514 안상준
202202602 손예진
202202487 박혜연
조은선 교수님