WEEK6-코드 난독화 도구 제작

유스 케이스(Use Case)

종합설계1

컴퓨터융합학부

노형우 | 손지웅 | 조인우

지도 교수 : 조은선

목차

01 연구 배경

SW 산업은 지식 재산권 침해 문제에 지속적으로 직면
LLM 활용한 역난독화 기술의 등장 → 기존 난독화 기법의 효과 저하
보다 정교하고 진화된 난독화 기술 필요

기존 난독화

특정 패턴에 기반해 적용
숙련된 분석자, AI 기반 도구에 의해
우회될 가능성

구조적으로 해석을 방해하는
기술적 접근이 요구됨

02 연구 목적

- **목적 1** 역공학 및 AI 기반 코드 분석 기술에 대한 방어 수단 제공
- **목적 2** 고도화된 코드 보호 효과 검증
- **목적 3** 고성능 복원도구에 대한 저항성 확보
- **목적 3** 다양한 언어와 플랫폼에 적용 가능한 범용 프레임 워크 구축

02 연구 목적

파스트리 분석(ANTLR)

IR 수준의 구조적 코드 변환 (LLVM)

→ 효과성 검증 →

실용적, 유의미한 난독화 도구

03 연구 질문/가설

RQ1. AI 기반 복원 도구에 대한 저항성을 얼마나 향상 시키는가?

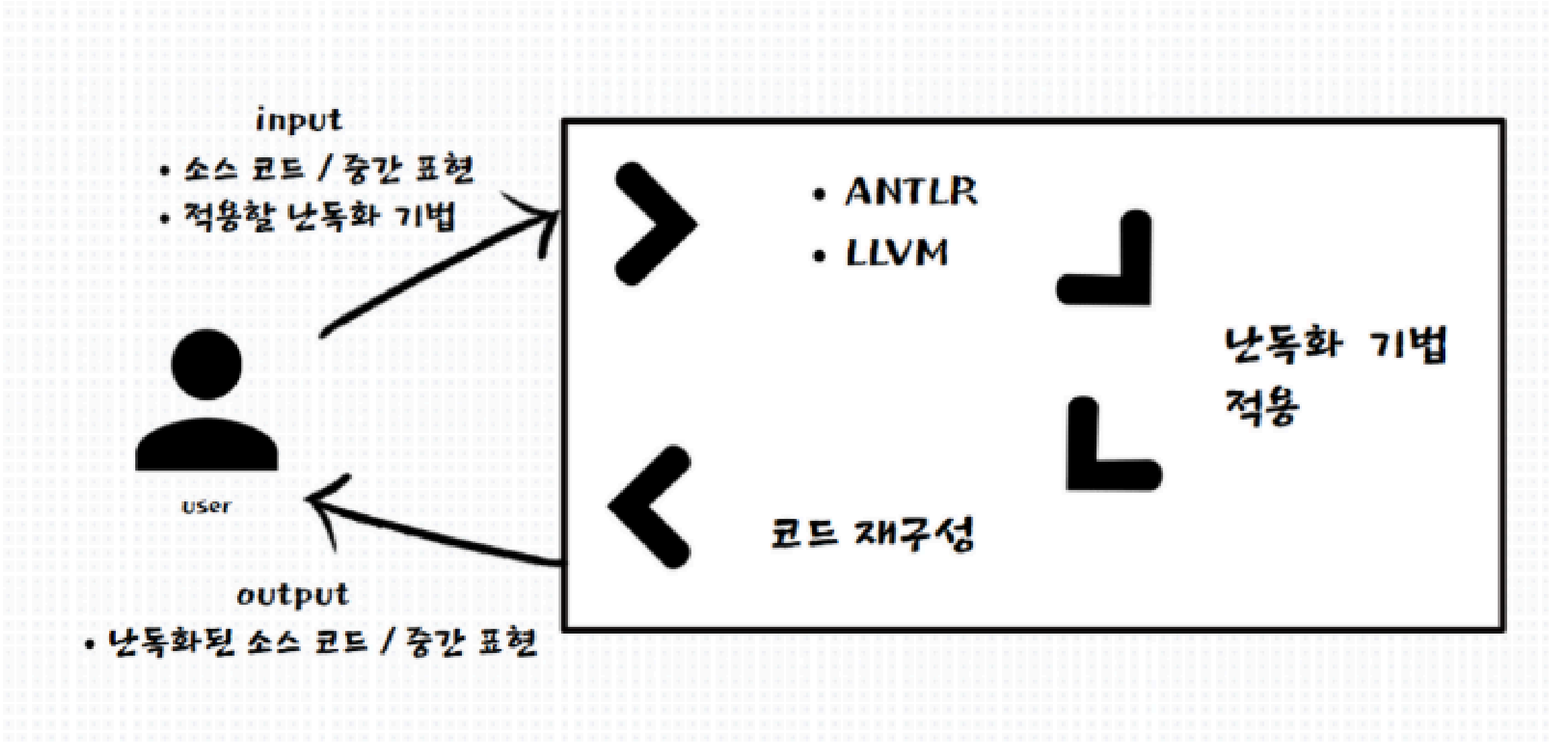
H1. AI 기반 분석 도구에 대한 복원 저항성을 유의미하게 향상시킬 것

RQ2. 소스코드 수준 난독화와 IR 수준 난독화 중
어느 방식이 실행 성능과 보안성 균형 측면에서 더 효과적인가?

각각의 적용 대상과 상황에 따라
보안성과 성능 측면에서 상이한 효과를 보일 것입니다.

04 다이어그램

소프트웨어 사용 사례



04 다이어그램

문제 해결에 대한 사용 사례

- GPT 등 LLM의 발전(역난독화 용이)
- 반복적인 난독화 방식
- 기존 도구의 낮은 복원 저항성

“코드 난독화 도구 제작“

기존 도구의 정형 패턴 사용으로 인해
AI 복원 도구에 쉽게 분석되어 보안 취약

알고리즘 보호가 필요한
기업용 소프트웨어,
사이드 프로젝트 코드 보호,
학술 실험용 보안 연구

05 활용 사례

소프트웨어 활용 사례

주요 Actor	기업 내부 알고리즘, 소스 코드 보안을 위해 난독화 도구를 사용하는 실무자
주요 기능	• 소스 코드 및 중간 표현 난독화 수행 • 코드 복원 저항성 향상 • 다양한 난독화 방식 제공
구성 요소	• 소스/IR 난독화 처리 엔진 • 난독화 방식 선택기 • 웹 기반 사용자 인터페이스로 구성된 자동화 코드 난독화 도구
입력 데이터	난독화 대상 소스 코드 또는 IR
출력 데이터	난독화가 완료된 소스 코드 또는 IR

05 활용 사례

소프트웨어 활용 사례

Data Flow	1) 사용자가 웹에 코드 업로드 2) 난독화 방식 선택 3) 해당 엔진에서 난독화 수행 4) 난독화된 코드 반환
외부 시스템 연계	API, 외부 평가 모듈(GPT 등)을 통한 복원 테스트 또는 품질 검증 수행

05 활용 사례

문제 해결에 대한 사용 사례

핵심 문제

기존 난독화 도구가 정형화된 패턴을 사용하여
AI 기반 복원 도구(LLM, 디컴파일러 등)에 의해 쉽게 분석되는 보안 취약성

직접 요인

- 반복적인 난독화 방식
- 기존 도구의 낮은 복원 저항성
- 특정 언어 및 플랫폼에 한정된 적용 범위

간접 요인

GPT 등 LLM을 이용해 코드 복원 시도가 누구나 가능

활용 맥락

알고리즘 보호가 필요한
기업용 SW, 사이드 프로젝트 코드 보호, 학술 실험용 보안 연구

06 질문과 답변 Q & A

궁금한 점이 있다면 자유롭게 질문 바랍니다 !

THANK YOU

감사합니다