WEEK8-코드 난독화 도구 제작

시퀀스 다이어그램 Sequence Diagram

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 4** 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?

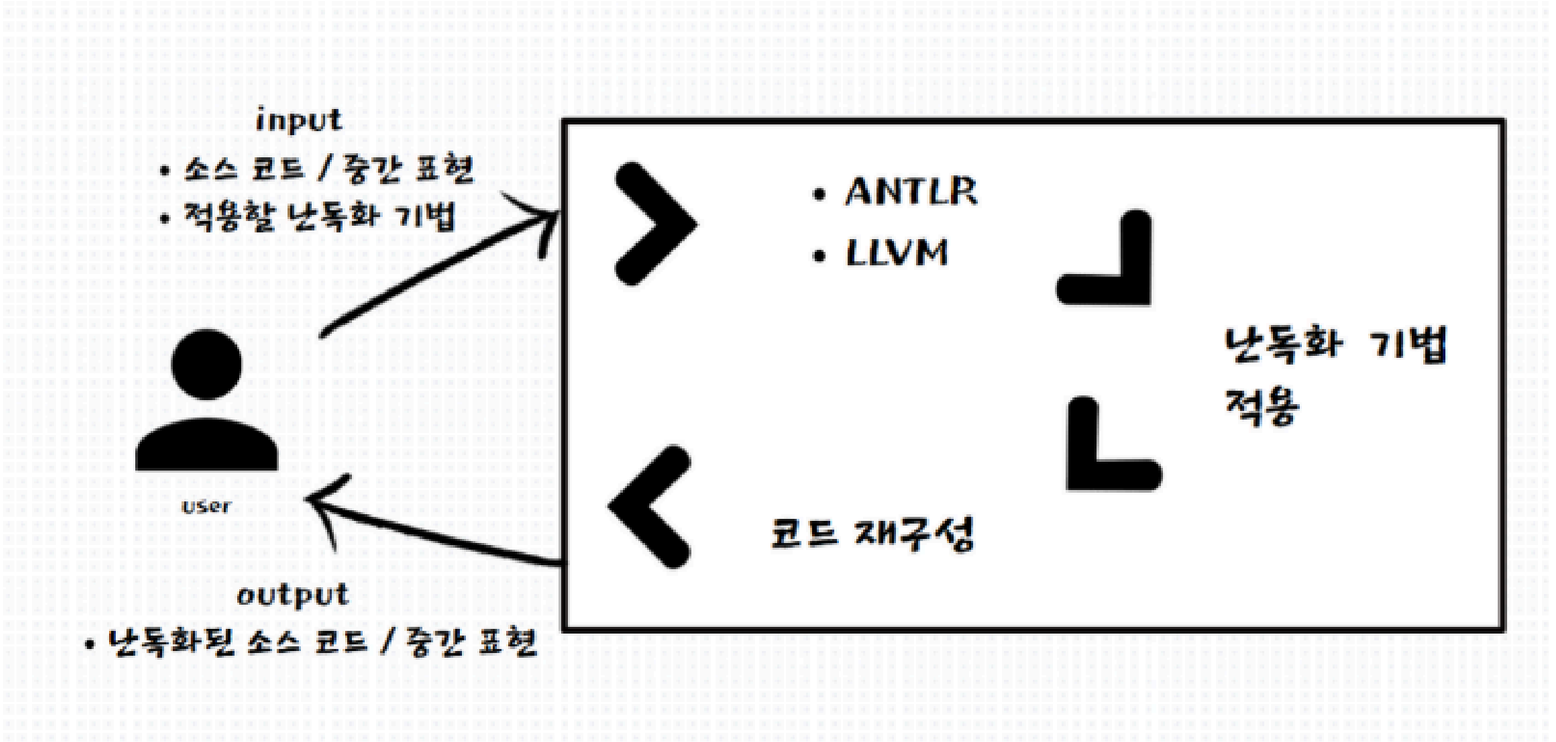
H1. AI 기반 분석 도구에 대한 복원 저항성을 유의미하게 향상시킬 것

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

H2. 각각의 적용 대상과 상황에 따라
보안성과 성능 측면에서 상이한 효과를 보일 것입니다.

04 유스케이스

소프트웨어 사용 사례



04 유스케이스

문제 해결에 대한 사용 사례

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

“코드 난독화 도구”

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 시퀀스 다이어그램

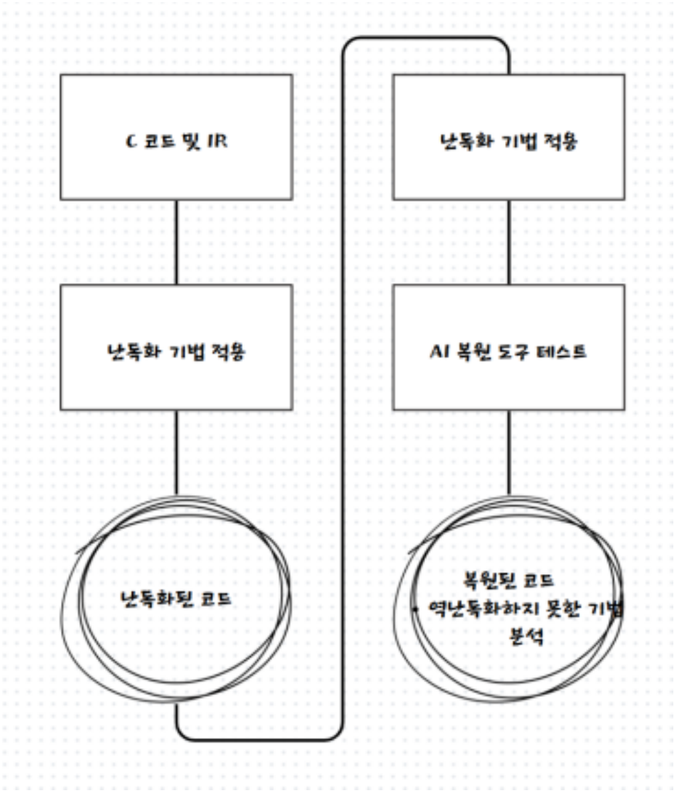
H1. AI 기반 분석 도구에 대한 복원 저항성을 유의미하게 향상시킬 것

H2. 각각의 적용 대상과 상황에 따라
보안성과 성능 측면에서 상이한 효과를 보일 것입니다.

핵심 문제 정의

LLM 기반 분석 도구와 고도화된 리버스 엔지니어링에 대응하기 위해,
소스 코드 및 중간 표현(IR) 수준에서 문법적 구조와 실행 흐름을 교란하는 컴파일러 기반 난독화 기법을 설계하고,
구조적 복원 저항성을 확보하는 범용 난독화 프레임워크를 구현한다.

05 시퀀스 다이어그램 해결 방법의 알고리즘 순서도

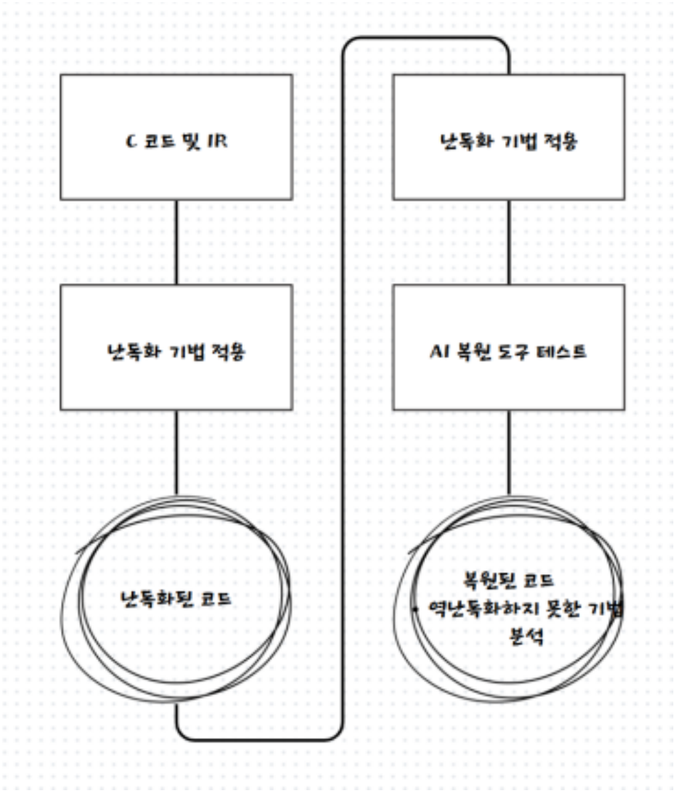


1. 입력 데이터 수집
   - 사용자 소스 코드 or LLVM 중간 표현(IR)

2. 분석 대상 분류
   - ANTLR 기반 : C 코드
   - LLVM 기반 : 중간 표현(IR)

3. 난독화 기법 적용
   - ANTLR : 식별자 치환, dead code 삽입, 조건 분기 왜곡 등
   - LLVM : control flow flattening, opaque predicate 등

05 시퀀스 다이어그램 해결 방법의 알고리즘 순서도



4. 코드 재구성 및 출력
   - 난독화된 결과물 생성
   - 원래 코드와 기능 동등성을 유지

5. AI 복원 도구에 대한 테스트
   - GPT/LLM 기반 코드 복원 도구에 입력
   - 복원율 및 실행 시간 분석

06 질문과 답변 Q & A

궁금한 점이 있다면 자유롭게 질문 바랍니다 !

THANK YOU

감사합니다