PROJECT DOCUMENT

Development of C Code Obfuscation Techniques

Research Proposal

Project Name	Code Obfuscation Tool Development

15 조

202002562 조인우
202002508 손지웅
201902686 노형우

지도교수: 조은선 교수님 (서명)

Document Revision History

Rev#	Date	Affected Section	Author
1	2025/03/13	Initial Draft	조인우
2	2025/03/14	Literature review	손지웅
3	2025/03/15	Plan Establishing	노형우

Table of Contents

목차

1.연구 주제 이름

C 언어를 위한 코드 난독화 기법 탐구: 새로운 접근법과 언어 확장 가능성

2.연구 배경 및 관련 연구

소프트웨어 보안은 역공학 공격과 불법 복제로부터 프로그램을 보호하는 중요한 연구 분야이다. 소프트웨어가 배포되는 과정에서 악의적인 사용자가 소스 코드를 분석하거나 변조할 경우 보안 취약점이 발생할 수 있다. 이를 방지하기 위해 난독화 기술이 개발되었으며, 난독화는 프로그램의 기능을 유지하면서도 코드를 이해하기 어렵게 변환하는 기법이다. 기존 연구들의 한계를 분석한 결과, 보다 강력한 소프트웨어 보호를 위해서는 소스 코드 수준에서 효과적인 난독화 기법이 필요하다. 특히, 기존 난독화 기법이 특정 환경이나 언어에 종속되는 경우가 많아, 다양한 프로그래밍 언어에서 적용 가능한 범용적인 난독화 기술의 개발이 요구된다. 이에 따라 향후 연구에서는 소스 코드 기반 난독화의 난이도를 더욱 높이는 기법을 도입하고, 정적 분석 및 디컴파일을 효과적으로 방어할 수 있는 기술을 개발하는 것이 필요하다.

3.프로젝트 수행자의 의도

본 프로젝트는 코드 난독화 기술의 한계를 보완하고, 더 강력하고 효율적인 난독화 방법을 개발하는 것을 목표로 한다. 기존의 코드 난독화 기법들이 가지는 취약점을 해결하고, 새로운 기법을 제안함으로써 코드 보안 기술을 발전시키는 데 기여하고자 한다. 또한, 난독화 도구의 범용성을 높여 다른 프로그래밍 언어에도 적용 가능하도록 확장한다면, 이는 다양한 산업에서 활용될 수 있는 중요한 기술이 될 것이다.

4.탐구 내용 및 기대 결과

프로젝트 기간 동안 기존의 코드 난독화 기법을 분석하고, 새로운 난독화 방법을 고안할 예정이다. C 언어를 주요 대상으로 삼되, 다른 프로그래밍 언어로 확장 가능한 난독화 기법을 테스트할 계획이다. 구체적으로는 컴파일러의 코드 변환 기술과 IR(Intermediate Representation) 및 IR 조작 도구를 활용하여, 코드의 가독성을 떨어뜨리면서도 기능은 그대로 유지하는 난독화 기법을 개발할 것이다. 또한, 난독화 기법의 성능에 미치는 영향을 최소화하고, 리버스 엔지니어링을 어렵게 만드는 효과적인 전략을 도출할 예정이다. 이를 위해 코드 분석 도구를 사용하여 난독화 기법의 강도를 평가하고, 난독화된 코드의 실행 속도와 보안성의 균형을 맞추는 최적화 방법을 모색할 것이다. 최종적으로, 다양한 테스트와 실험을 통해 개발된 난독화 방법이 기존 기법들보다 뛰어난 성능과 보안성을 제공하는지 검증할 계획이다.

5.프로젝트 관련 학습 계획

학습할 내용	기간	역할 분담
소프트웨어 난독화 개요 및 기존 연구 분석	3/14 ~ 3/20	조인우
Opaque Predicates & MBA 난독화 기법 조사	3/21 ~ 3/27	손지웅, 노형우
ANTLR을 활용한 코드 파싱 및 식별자 난독화 조사	3/28 ~ 4/10	조인우, 손지웅
Inline Assembly 활용 난독화 기법 조사	4/4 ~ 4/10	노형우
난독화 도구 개발 환경 설정 및 기본 구조 설계	4/11 ~ 4/17	조인우, 손지웅, 노형우
기본 난독화 기능 구현 (Opaque, MBA, 식별자 난독화)	4/18 ~ 5/1	조인우, 손지웅, 노형우
다층 난독화 적용 기법 연구 및 성능 평가	5/2 ~ 5/29	조인우, 손지웅, 노형우
실험 및 기존 난독화 도구와 비교 분석	5/30 ~ 6/12	조인우, 손지웅, 노형우
논문 작성 및 최종 보완	6/13 ~ 7/3	조인우, 손지웅, 노형우

6.연구 일정 계획

조사할 내용	기간	역할 분담
소프트웨어 난독화 개요 및 기존 연구 분석	3/14 ~ 3/20	조인우
기존 난독화 도구(OBFUS, OLLVM 등) 조사	3/21 ~ 3/27	손지웅
Opaque Predicates 난독화 기법 조사	3/21 ~ 3/27	노형우
MBA 난독화 및 활용 사례 조사	3/28 ~ 4/3	조인우
ANTLR을 활용한 코드 파싱 조사	4/4 ~ 4/10	손지웅
식별자 난독화 및 Uglyfier 조사	4/4 ~ 4/10	노형우
Inline Assembly 난독화 기법 조사	4/11 ~ 4/17	조인우
다층 난독화(중첩 난독화) 연구 조사	4/18 ~ 5/1	손지웅, 노형우
난독화 적용 후 성능 평가 방법 조사	5/2 ~ 5/15	조인우

Related Work Summary Table

번호	연구 제목(저자)	저널/컨퍼런스(연도)	주요 내용 요약	주요 인사이트
1	모바일 게임 보안을 위한 게임내 데이터 난독화에 관한 연구(김효남)	한국컴퓨터정보학회 동계학술대회 논문집, 25(1), 2017.1	국내 모바일 게임 시장은 약 4조 원 규모로 성장했으며, 사용자의 하루 평균 게임 시간도 43분으로 증가하고 있다. 이에 따라 모바일 게임이 사이버 범죄의 주요 대상이 되면서 해킹 툴의 등장과 공유가 활발해져 보안 문제가 심각해졌다. 본 연구에서는 게임 내 데이터 난독화(Obfuscation) 기술을 활용하여 모바일 게임의 원본 소스 데이터를 보호하는 방법을 제안하며, 난독화와 Anti-decompile 기법을 주요 보안 기술로 적용한다. 또한, 대표적인 난독화 도구(Dotfuscator, Crypto Obfuscator, Unity3D Obfuscator)를 소개하고, 모바일 게임의 캐시 데이터를 보호하기 위한 난독화 기법 적용 방법을 코드 예제와 함께 설명한다.	모바일 게임 시장이 빠르게 성장하면서 보안 위협도 증가하고 있으며, 해킹 방지를 위해 데이터 난독화와 Anti-decompile 기법이 필수적이다. 이를 위해 대표적인 난독화 도구를 활용할 수 있으며, 모바일 게임의 캐시 데이터를 보호하는 실용적인 방법이 존재한다.

2	소프트웨어 보안을 위한 난독화 기술 동향(이경률, 육형준, 임강빈, 유일선)	정보과학회지 (2016.1)	소프트웨어 불법 복제가 심각한 문제로 대두되면서, 기존의 시리얼 키 방식 등 보안 기법이 역공학 공격에 취약한 한계를 보이고 있다. 공격자는 역공학 기술을 활용해 소프트웨어의 동작을 분석하고, 기능을 우회하거나 악성코드를 삽입할 수 있다. 이를 방어하기 위한 핵심 기술인 난독화(Obfuscation)는 코드를 변형하여 해석을 어렵게 만드는 방법으로, 배치 난독화, 자료 난독화, 제어 난독화, 방지 난독화로 구분된다. 배치 난독화는 식별자 변환 및 주석 제거를 통해 물리적 구조를 변경하고, 자료 난독화는 변수 분할 및 데이터 인코딩을 활용해 데이터 해석을 어렵게 한다. 제어 난독화는 루프 변형 및 제어 흐름 재구성을 통해 분석을 방해하며, 방지 난독화는 디버거 탐지 및 PE 구조 변형 등을 활용해 디버깅 및 디컴파일링을 차단한다. 또한, 패킹 및 가상화 기술을 병행하면 실행 방식을 변형하여 역공학을 더욱 어렵게 만들어 소프트웨어 보안을 강화할 수 있다.	기존의 시리얼 키 방식 등 전통적인 보안 기법은 역공학 공격에 취약해 소프트웨어의 동작 분석이나 악성코드 삽입을 허용할 수 있다. 이를 방어하기 위해 난독화(Obfuscation) 기술이 중요한 역할을 한다. 난독화는 소프트웨어의 코드를 변형하여 해석을 어렵게 만들며, 배치 난독화, 자료 난독화, 제어 난독화, 방지 난독화 등 다양한 유형으로 구분된다. 또한, 패킹 및 가상화 기술과 함께 사용하면 역공학을 더욱 어렵게 만들어 소프트웨어 보안을 강화할 수 있다.
3	OBFUS: An Obfuscation Tool for Software Copyright and Vulnerability Protection(Seoyeon Kang, Sujeong Lee, Yumin Kim,	11th ACM Conference on Data and Application Security & Privacy (CODASPY '21), 2021. 4. 26-28	OBFUS는 웹 기반 난독화 도구로, 고급 프로그래밍 언어(C)와 저급 프로그래밍 언어(x86 어셈블리)에 대한 난독화를 지원한다. 사용자는 C 코드를 업로드하고 다양한 난독화	OBFUS는 웹 기반 난독화 도구로, C와 x86 어셈블리와 같은 고급 및 저급 프로그래밍 언어에 대한 난독화를 지원하며, 소스 코드와 바이너리 난독화 모두 가능하다. 이를 통해

	Seong-Kyun Mok, Eun-Sun Cho)		옵션(불투명 조건, 코드 구조 수정, 변수명 변경 등)을 선택하여 소스 코드 난독화를 적용할 수 있으며, LLVM IR을 활용해 실행 파일을 역컴파일하고 난독화 후 다시 실행 가능한 바이너리로 변환하는 바이너리 난독화도 지원한다. OBFUS의 난독화 기법은 수학적 표현 변환(MBA), 불투명 조건, 변수명 변경, 가상화 실행 등을 포함하며, 기존 난독화 도구인 ADVobfuscator와 OLLVM에 비해 웹 기반으로 접근성과 사용성이 뛰어나고, 소스 코드 난독화까지 지원하는 차별점을 가지고 있다.	사용자는 다양한 난독화 옵션을 적용하여 소프트웨어의 보안을 강화할 수 있다. OBFUS는 수학적 표현 변환, 불투명 조건, 변수명 변경, 가상화 실행 등의 기법을 제공하고, 기존의 ADVobfuscator와 OLLVM과 비교하여 웹 기반으로 접근성이 뛰어나며 소스 코드 난독화도 지원하는 점에서 차별화된다.